EMBEDDED

NOVEMBRE 2014 54

contradata®

LA COPERTINA EMBEDDED

Contradata abbraccia la filosofia 'convertibile' Cincoze

SPECIALE

Ide, un tool versatile e indispensabile

Sensori industriali ottici

Supplemento a Elettronica oggi n° 441 - Novembre - In caso di mancato recapito inviare al CMP/CPO di Roserio-Milano per la restituzione al mittente previo pagamento resi

A CHI SI RIVOLGE

L'evento si rivolge a manager, tecnici, progettisti, specialisti e opinion leader che operano nel mondo produttivo, a OEM, costruttori di impianti e linee di produzione, system integrator, utilizzatori finali.

I LABORATORI

Interessante modalità di apprendimento. I partecipanti potranno imparare a utilizzare i prodotti delle aziende avvalendosi della guida di tecnici esperti.

I WORKSHOP

Seminari tecnici tenuti dalle aziende espositrici della durata di 30 minuti ciascuno.

LA MOSTRA

Esposizione a cura delle aziende partecipanti. Sarà possibile verificare l'attuale offerta commerciale.

PER ADERIRE

Visita il sito **ma.mostreconvegno.it.** per partecipare ai seminari, alla mostra e ai laboratori. La partecipazione è gratuita. Tutta la documentazione sarà disponibile on-line il giorno stesso della manifestazione.

GIOVEDÌ 11
Circonva

Quest
pur
del **Packa**
alle
Food

CON LA COLLABORAZIONE DI:

progettare EO elettronica mo TECH PLUS.it EMBEDDED

ORGANIZZATO DA:

AUTOMAZIONE E STRUMENTAZIONE IAO Field & Netw

E AUTOMATION

DICEMBRE 2014 IBM CLIENT CENTER
allazione Idroscalo 20090 Segrate MI

t'anno **Machine Automation**
nterà i riflettori sul mondo
aging con particolare riferimento
e applicazioni per i settori
& Beverage e **Life Science**.

FOCUS PACKAGING

CON IL PATROCINIO DI:

ANIE AUTOMAZIONE

A.N.I.P.L.A. ASSOCIAZIONE NAZIONALE ITALIANA PER L'AUTOMAZIONE

IBM

EXPO MILANO 2015

FIERA MILANO MEDIA

Fiera Milano Official Partner

ma.mostreconvegno.it
machineautomation@fieramilanomedia.it
Ufficio commerciale: 335 276990
segreteria organizzativa: 02 49976533
contatti

CYBERSCREEN®

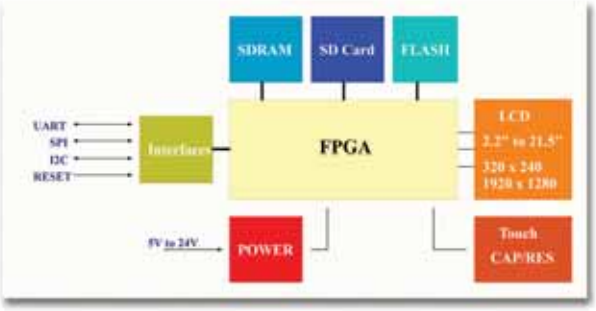
THE SMART TOUCH SCREEN FOR THE IND

Solutions Architecture

CYBERSCREEN® is a ***cost-effective & easy solution*** for any industrial application where ***HMI*** is necessary. Its hardware has the ability to interface in single-ended or LVDS many kinds of displays, making it a valid solution for the industrial enviroment. The display technology that can be used are the standard ***TFT LCD*** (from 2.2" to 21.5") and the monochrome ***E-Paper*** (from 1.44" to 10.4"). It is a versatile system that can be handle resistive or capacitive touch screens. This smart display is ***instant-on*** (less than 2 seconds) and is able to communicate with external systems through programmable ***UART***, ***SPI***, ***I2C***, ***CAN***, ***ETHERNET***, ***USB*** and ***WiFi*** interfaces (***KNX*** on request). The software applications and data can be stored into ***SD card*** and/or ***Flash chip*** directly on board. **CYBERSCREEN**® can be based on ***FPGA*** solution, without an Operating System and/or ***ARM***™ processors, with Operating Systems.

Embedded HMI-on-chip FPGA solution

The ***FPGA*** **CYBERSCREEN**®'s firmware is based on IQ-Display, which is a ***compact FPGA*** solution for rapid developement and deployment of embedded graphical Human-Machine Interfaces (***HMI***s). The solution offers all the functionality required to drive the display, to render the graphics and to make the embedded visualization. It is scalable from small size QVGA to large Full HD displays, as well as a wide variety of touch screens and system interfaces.
The ***FPGA*** **CYBERSCREEN**® is an ***HMI-on-chip without the need of an Operating System***, neither any line of C code nor software complexity to use ***openGL*** library. The built-in graphical engine (IQ-Engine) interprets an integrated interface project file to visualize and modify a set of values shared with the host application, allowing easy integration of the user interface. Using an FPGA brings an absolute flexibility of the solution to the user, supporting the widest possible range of displays, memories or system interfaces.



FPGA Interface Design

The graphical user interface can be designed simply and quickly in a **what-you-see-is-what-you-get** mode, and deployed to the hardware without the need to use complex SW architecture, write C code, or use an operating system.
The IQ-Editor application allows easy inclusion and manipulation of high-end graphical elements, managing multiple graphics levels and transparencies, and creating unlimited levels of menu structure, graphics, and details. Standard objects such as buttons, sliders and bar-graphs are supported.

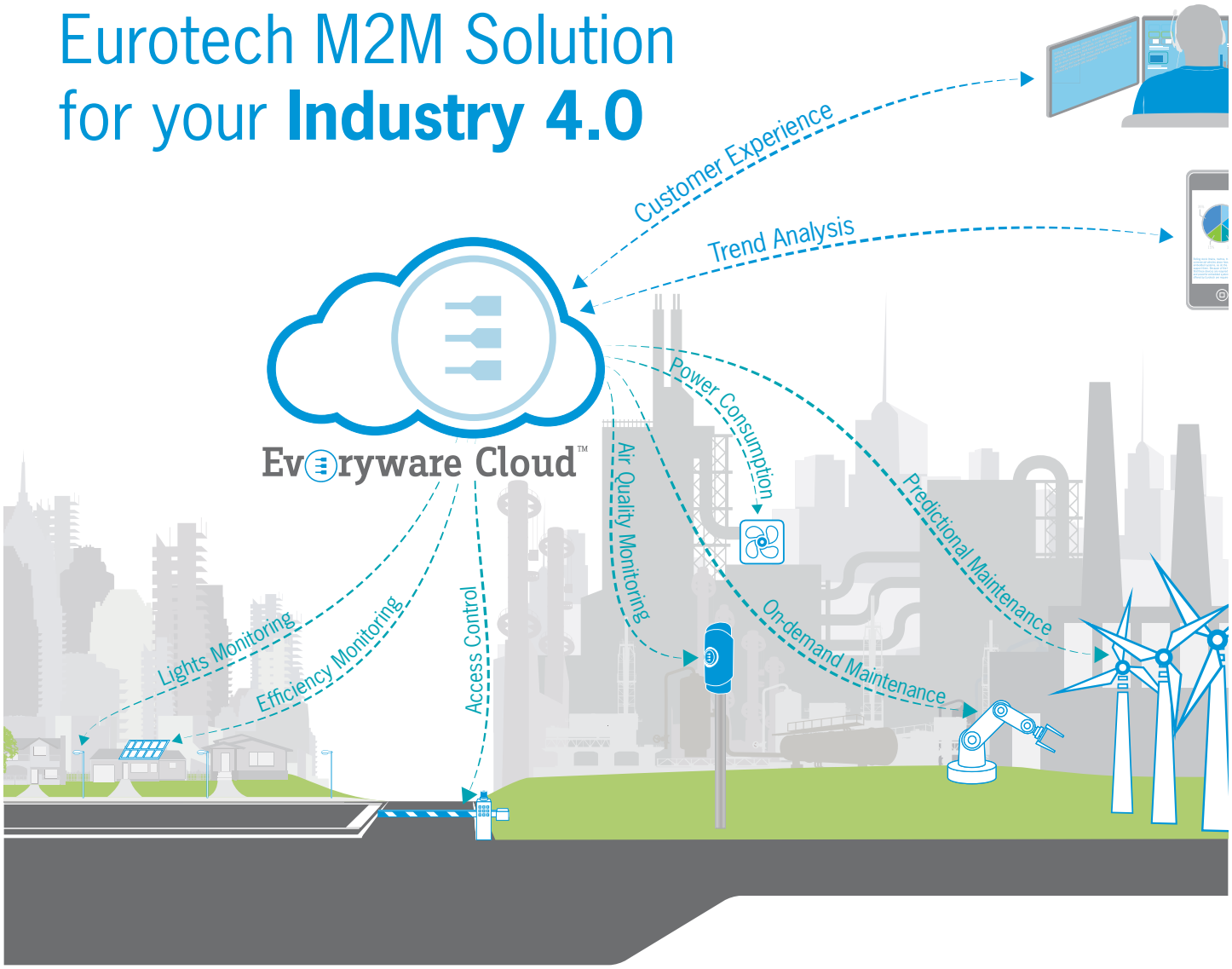
Embedded HMI ARM™ solution

The ***ARM***™ **CYBERSCREEN**®'s hardware is based on a standard cores ***A5***, ***A8*** and ***A9*** solution for rapid developement and deployment of embedded graphical Human-Machine Interfaces (***HMI***s). The solution offers all the functionality required to drive the display, the touch screen & standard interface with the eviropment. Can use some standard OS, like to RTOS, Linux, Android & Win CE and is possible to develope many APP with standard and open source software how QT, VC, VB and many others.

EuroLink Systems
MADE IN ITALY

EuroLink Systems srl
Via Piedicavallo, 51 - 2/B - 00166 Rome (ITALY)
Tel. +39.06.619140.1 - Fax. +39.06.619140.20
www.eurolinksystems.com - info@eurolinksystems.com

Eurotech M2M Solution for your **Industry 4.0**



Eurotech helps customers connect industrial equipment and sensors seamlessly and securely to Enterprise applications through **Everyware Cloud™**, a **M2M Integration Platform.** It offers out of the box functionalities like:

- Device operation and management
- Device application and lifecycle management
- Real-time device/connection status
- Support for industrial protocols
- Easy integration with enterprise applications
- Real-time data analysis and historical data
- Aggregated Real-time data streams from devices

www.eurotech.com

EUROTECH
Imagine. Build. Succeed.

Europe, Middle East and Africa
sales.emea@eurotech.com

Latin America
sales.la@eurotech.com

North America
sales.na@eurotech.com

Asia Pacific
sales.ap@eurotech.com

For your local contact please refer to:
www.eurotech.com/contacts

SÌ

SONO SEMPRE **PUNTUALI NELLE** CONSEGNE?

HANNO UNA **VASTA GAMMA** DI CONNETTORI?

NO

NON PROSEGUIRE

SÌ

SÌ

POSSO ORDINARE QUELLO CHE MI SERVE NELLE QUANTITÀ DI CUI HO BISOGNO?

NO

SONO DISTRIBUTORI AUTORIZZATI?

SÌ

SU CHI POSSO FARE AFFIDAMENTO PER I PRODOTTI **TE CONNECTIVITY** DI CUI HO BISOGNO?

Puoi fare affidamento su di noi per ciò di cui hai bisogno.

Scegliere il distributore adatto alle tue esigenze è importante come scegliere il giusto prodotto. RS ti offre più di 22.000 prodotti TE Connectivity disponibili a magazzino. Nessun minimo d'ordine con consegna in 24 ore per ordini pervenuti prima delle ore 18.

it.rs-online.com

TE connectivity

Authorized Distributor

RS

SOMMARIO

8 SI PARLA DI...
9 EDITORIALE

LA COPERTINA EMBEDDED
10 Contradata abbraccia la filosofia 'convertibile' Cincoze - **Giorgio Fusari**

IN TEMPO REALE
14 La combinazione M2M e IoT spinge il business - **Francesca Prandi**
19 Analizzatore di rete vettoriale integrato in un unico slot Pxi - **Maurizio Di Paolo Emilio**
22 Robustezza militare con componenti commerciali - **Lucio Pellizzari**
26 Internet of Things: sfide e opportunità - **Alexander Damisch**
29 Computer rugged orientati alle applicazioni - **Massimo Fiorini**
31 Le prospettive di PC/104 nell'era di Internet of Things - **Lucio Pellizzari**

SPECIALE
33 Ide, un tool versatile e indispensabile - **Francesco Ferrari**
37 Sensori industriali ottici - **Lucio Pellizzari**

HARDWARE
42 Tecnologie basate su Internet per le smart grid - **Jouni Kujala**
46 Reti industriali: a ciascuno il suo protocollo - **Silvano Iacobucci**
51 Sistemi embedded multi-core - **Maurizio Di Paolo Emilio**
54 Computer industriali - **Lucio Pellizzari**
58 L'acquisizione dei dati - **Francesco Ferrari**
60 Problematiche per la messa a punto di Small Form Factor rugged con parti commerciali - **Lucio Pellizzari**

SOFTWARE
63 L'impatto sull'affidabilità dei sistemi della gestione remota basata su cloud - **Dirk Finstel**
69 C++: la 'grammatica' per un codice senza errori (II parte) - **Giorgio Fusari**
73 La protezione dei sistemi IoT dagli attacchi persistenti - **Avishai Ziv**
76 Rtos, l'evoluzione della specie - **Giorgio Fusari**
80 SO embedded nell'era IoT, fra tradizione ed evoluzione - **Stefano Rinaldi**

84 Prodotti

In copertina:

Contradata ha da poco arricchito la propria offerta grazie all'accordo commerciale stipulato con la società taiwanese Cincoze, che si distingue per la costruzione di particolari tipologie di panel PC, touch monitor e sistemi embedded. Cincoze si colloca sul mercato come fornitore di sistemi nel comparto dell'industrial computing, progettando, costruendo e commercializzando prodotti altamente ingegnerizzati e innovativi. Tra questi spicca la soluzione modulare 'Convertible Display System' (CDS), che la società ha inventato e brevettato a livello mondiale e che caratterizza tutti i panel PC e monitor della gamma.

Contradata
Via Solferino 12
20090 MB
Tel +39 039 2301492
Fax +39 039 2301489
info@contradata.it
www.contradata.it

COMING SOON ON www.elettronica-plus.it

Ottimizzare il design termico dei dispostivi elettronici per networking e telecom - John Parry

INDICE INSERZIONISTI

SOCIETÀ	PAG.
CONTRADATA	I COPERTINA
EUROLINK SYSTEMS	II COPERTINA
EUROTECH	5
FENWAY EMBEDDED SYSTEMS	65
GOMA ELETTRONICA	61
HMS INDUSTRIAL NETWORKS	9
LAUTERBACH	67
MC' TRONIC	25
MESSE FRANKFURT – SPS 2015	41
NATIONAL INSTRUMENTS	IV COPERTINA
NURNBERG MESSE	27
RS COMPONENTS	6
TECNOLOGIX	INSERTO
WIBU SYSTEMS	47

SI PARLA DI...

SOCIETÀ	WWW	PAG/WEB
AAEON TECHNOLOGY EUROPE	www.aaeon.eu	54
ADLINK TECHNOLOGY	www.adlinktech.com	14-54-60-63
ADVANTECH	www.advantech.it	84
AEC COUNCIL	www.aecouncil.com	22
ALTERA	www.altera.com	42
AMPHENOL	www.amphenol.com	22
ANALOG DEVICES	www.analog.com	33
ARM	www.arm.com	31-33
ATMEL	www.atmel.com	33
AVX	www.avx.com	22
B&R AUTOMAZIONE INDUSTRIALE	www.br-automation.com	58
CAMBIUM NETWORKS	http://www.cambiumnetworks.com/	22
CINCOZE	http://www.cincoze.com/	10-54
CONGATEC	www.congatec.com	84
CONNECT TECH	www.connecttech.com	60
CONTRADATA	www.contradata.it	10-29-54
CYPRESS SEMICONDUCTOR	www.cypress.com	84
DEFENCE TECHNOLOGY INFORMATION	www.dtic.mil/	22
ENEA EMBEDDED TECHNOLOGY	www.enea.com	76
EUROLINK SYSTEMS	www.eurolinksystems.com	54
FLEXIBILIS OY	http://www.flexibilis.com/	42
FREESCALE SEMICONDUCTOR	www.freescale.com	33-51
GE INTELLIGENT PLATFORMS	www.ge-ip.com	54
GOMA ELETTRONICA	www.gomaelettronica.it	54
IFM ELECTRONIC	www.ifm-electronic.com	46
INNOVATIVE INTEGRATION	www.innovative-dsp.com	54
KEMET	www.kemet.com	22
KEYSIGHT TECHNOLOGIES	www.keysight.com	19
LINUX	www.linux.org	76
LINUX FOUNDATION	www.linuxfoundation.org	31
LYNX SOFTWARE TECHNOLOGIES	http://www.lynx.com/	73
MAXIM INTEGRATED	www.maximintegrated.com	33
MENTOR GRAPHICS	www.mentor.com	76
MICROSCAN	www.microscan.com/it	37
MICROSOFT	www.microsoft.com	58
MPL	www.mpl.ch	54
NEOUSYS	www.neousys-etch.com	54
OMRON ELECTRONICS	www.omron.com	37
ON SEMICONDUCTOR	www.onsemi.com	37
PANASONIC ELECTRIC WORKS IT	www.panasonic-electric-works.it	84
PC/104 CONSORTIUM	www.pc104.com	31
PEPPERL+FUCHS	www.pepperl-fuchs.it	37
PERFECTRON	http://www.perfectron.com/	29
PHOENIX CONTACT	www.phoenixcontact.it	46
RENESAS ELECTRONICS EUROPE	www.renesas.com	33
SAMSUNG ELECTRONICS	www.samsung.com	33
SENSOPART	www.tritecnica.it	37
SISTEMI AVANZATI ELETTRONICI	www.sisav.it	54
SPECIM	www.specim.fi	37
SPECTRIS	www.spectris.com	37
STMICROELECTRONICS	www.st.com	33
SYSLOGIC GROUP SWITZERLAND	www.syslogic.ch	54
TATTILE	www.tattile.com	37
TELIT COMMUNICATIONS	www.telit.com	14
TEXAS INSTRUMENTS	www.ti.com	33
TRITECNICA	www.tritecnica.it	37
VDC RESEARCH GROUP	www.vdcresearch.com	76
VODAFONE	www.vodafone.it	14
WIND RIVER	www.windriver.com	14-26

EMBEDDED
www.elettronica-plus.it
www.tech-plus.it
www.fieramilanomedia.it

Supplemento a Elettronica Oggi 441
ottobre 2014
Pubblicazione in diffusione gratuita

EXPO MILANO 2015
FIERA MILANO MEDIA
Fiera Milano Official Partner

Sede legale • Piazzale Carlo Magno, 1 - 20149 - Milano
Sede operativa ed amministrativa • SS. del Sempione, 28 - 20017 Rho (MI)
tel. +39 02 4997.1 fax +39 02 49976573 - www.tech-plus.it

Direzione
Giampietro Omati Presidente
Antonio Greco Amministratore Delegato
Publisher

Redazione
Antonio Greco Direttore Responsabile
Filippo Fossati Coordinamento Editoriale
filippo.fossati@fieramilanomedia.it - tel: 02 49976506
Paola Bellini Coordinamento di Redazione
paola.bellini@fieramilanomedia.it - tel: 02 49976501
Franco Metta Redattore
franco.metta@fieramilanomedia.it - tel: 02 49976500
Laura Varesi Segreteria
laura.varesi@fieramilanomedia.it - tel: 02 49976516

Collaboratori: Alexander Damisch, Maurizio Di Paolo Emilio, Francesco Ferrari, Dirk Finstel, Giorgio Fusari, Aldo Garosi (disegni), Silvano Iacobucci, Jouni Kujala, Lucio Pellizzari, Francesca Prandi, Avishai Ziv

Grafica e produzione
Franco Tedeschi Coordinamento grafici - impaginazione
franco.tedeschi@fieramilanomedia.it- tel: 02 49976569
Paola Queirolo - progetto grafico
paola.queirolo@fieramilanomedia.it - tel: 02 49976564
Alberto Decari Coordinamento DTP
alberto.decari@fieramilanomedia.it - tel: 02 49976561
Prontostampa Srl uninominale - Zingonia BG • Stampa
Nadia Zappa Ufficio Traffico
nadia.zappa@fieramilanomedia.it - tel: 02 49976534

Pubblicità
Giuseppe De Gasperis Sales Manager
giuseppe.degasperis@fieramilanomedia.it
tel: 02 49976527 - fax: 02 49976570-1

International Sales
U.K. – SCANDINAVIA – NETHERLAND – BELGIUM
Huson European Media
Tel +44 1932 564999 - Fax +44 1932 564998
Website: www.husonmedia.com
SWITZERLAND - IFF Media
Tel +41 52 6330884 - Fax +41 52 6330899
Website: www.iff-media.com
USA - Huson International Media
Tel +1 408 8796666 - Fax +1 408 8796669
Website: www.husonmedia.com
GERMANY – AUSTRIA - MAP Mediaagentur Adela Ploner
Tel +49 8192 9337822 - Fax +49 8192 9337829
Website: www.ploner.de
TAIWAN - Worldwide Service co. Ltd
Tel +886 4 23251784 - Fax +886 4 23252967
Website: www.acw.com.tw

Abbonamenti
N. di conto corrente postale per sottoscrizione abbonamenti:
48199749 - IBAN: IT 61 A 07601 01600 000048199749
intestato a: Fiera Milano Media SpA,
Piazzale Carlo Magno, 1 - 20149 - Milano
Si accettano pagamenti anche con Carta Sì, Visa, Mastercard, Eurocard
tel: 02 252007200 • fax: 02 49976572 • abbonamenti@fieramilanomedia.it

A.N.E.S. ASSOCIAZIONE NAZIONALE EDITORIA PERIODICA SPECIALIZZATA
Testata associata • **Associazione Nazionale Editoria Periodica Specializzata**

Fiera Milano Media è iscritta al Registro Operatori della Comunicazione n° 11125 del 25/07/2003.
Autorizzazione alla pubblicazione del tribunale di Milano n° 129 del 7/03/1978.

Tutti i diritti di riproduzione degli articoli pubblicati sono riservati.
Manoscritti, disegni e fotografie non si restituiscono. Embedded è supplemento di Elettronica Oggi.

EDITORIALE

Un futuro promettente per microprocessori e Gpu

Filippo Fossati
filippo.fossati@fieramilanomedia.it

Un recente report pubblicato da ResearchAndMarkets ha fatto il punto sui mercati di microprocessori, Gpu e periferiche, fornendo alcune utili proiezioni sul loro andamento per i prossimi anni. Le indicazioni sono positive: questi tre componenti essenziali per virtualmente ogni sistema elettronico, cresceranno nei prossimi anni a un tasso del 7,9% su base annua, raggiungendo entro il 2020 un fatturato pari a 128 miliardi di dollari. Per quanto riguarda microprocessori e Gpu, la parte del leone è ancora fatta da Intel con la sua linea di prodotti in architettura x86. La sua posizione di leadership è minacciata da Arm, che ha un ruolo di preminenza nel settore dei micro per smarphone e tablet. Non va dimenticato che quello dei dispositivi mobili, unitamente a reti cellulari, cloud computing e al più tradizionale settore automobilistico sono i driver che definiranno in misura maggiore l'evoluzione futura dei microprocessori. Per quanto riguarda invece le Gpu, le applicazioni che favoriranno la loro diffusione saranno, oltre alle console per videogiochi, quello della pubblicità e dell'animazione cinematografica.

Un fatto da tenere in considerazione è il progressivo declino dei personal computer tradizionali e la sempre maggiore diffusione di dispositivi mobili low-cost, due fattori che potrebbero influire in maniera significativa sui fatturati di alcune importanti aziende industriali.

Nulla di nuovo a livello geografico, dove la regione Asia Pacifico, Cina e Taiwan "in primis", continuerà a mantenere una posizione di indiscussa preminenza.

Filippo Fossati

HMS

Tre brand, un unico obiettivo:
Connecting Devices™

Anybus®

- Facile integrazione delle Reti fieldbus ed Ethernet industriali nei vostri dispositivi, basati sul concetto flessibile di Anybus chip, brick e module
- Soluzioni gateway per connettere reti diverse, in grado di supportare fino a 250 combinazioni di reti

www.anybus.it

IXXAT®

- Interfacce PC, moduli di IO, controllori, componenti e strumenti di campo per applicazioni di controllo ed analisi
- Componenti Safety per lo sviluppo semplice dei dispositivi di sicurezza, moduli, stack e servizi

www.ixxat.com

netbiter®

- La soluzione completa e pronta all'uso per la gestione remota dei dispositivi industriali

www.netbiter.com

HMS

HMS Industrial Networks srl
V.le Colleoni, 15 (Palazzo Orione, 2)
20864 Agrate Brianza (MB)
Tel.: +39 039 5966227 - Fax: +39 039 596623
E-mail: it-sales@hms-networks.com

www.anybus.it · www.ixxat.com · www.netbiter.com

Contradata abbraccia la filosofia 'convertibile' Cincoze

Gli innovativi moduli, panel PC, monitor e display dell'azienda taiwanese consentono di creare configurazioni molto flessibili. Da ottobre la gamma di prodotti è in distribuzione in Italia

Giorgio Fusari

Gli operatori, gli OEM, gli utenti del mondo e delle applicazioni embedded hanno tutti in comune l'esigenza di ottenere un'elevata affidabilità di funzionamento dei sistemi, soprattutto quando si tratta di prodotti come i PC industriali, o i panel PC. Al contempo, in questo ambito è anche importante poter contare sulla massima praticità di manutenzione e rapidità di risoluzione dei problemi, ad esempio quando occorre intervenire in seguito ad avarie dei sistemi, ed è necessario ridurre al minimo i tempi di fermo macchina.
Ugualmente importante, negli ambienti industriali, è salvaguardare e preservare gli investimenti tecnologici preesistenti, e realizzare applicazioni e configurazioni gestibili e aggiornabili in maniera pratica, per adeguarsi con flessibilità a necessità di business dinamiche.
Proprio con l'obiettivo di rispondere sempre meglio a queste e altre necessità e criticità del settore, Contradata – distributore di PC industriali e soluzioni embedded fra le principali realtà del panorama italiano – ha da poco arricchito la propria offerta attraverso l'acquisizione di una nuova gamma di interessanti prodotti, in distribuzione nel nostro paese già da ottobre. Tale strategia commerciale ha potuto concretizzarsi dopo un accordo commerciale con la società taiwanese Cincoze, che si distingue per la costruzione di particolari tipologie di panel PC, touch monitor e display.
Cincoze è un'azienda giovane, nata un paio d'anni fa, spiega Alessandro Damian di Contradata, ricordando però di avere, già da molti anni, un consolidato rapporto di conoscenza e collaborazione con i suoi fondatori. "Quest'azienda è nata grazie a un grande investimento, e i suoi prodotti sono stati esposti quest'anno, al Computex di Taipei. Conoscendo il nostro posizionamento come distributore di PC industriali, siamo la prima società a cui Cincoze ha pensato per la commercializzazione della propria gamma di soluzioni in Italia.

Fig. 1 - Il Convertible Display System brevettato da Cincoze

Con loro abbiamo avuto una serie di incontri e presentazioni, nei quali siamo rimasti decisamente colpiti da alcune particolari caratteristiche dei prodotti". E, sottolinea, questi ultimi segnano una svolta veramente importante a livello mondiale nelle soluzioni del settore: probabilmente, nessuno è riuscito a innovare così prodotti che, all'apparenza, sembrerebbero difficilmente innovabili.

Panel PC e monitor convertibili: scalabilità, modularità e facilità di manutenzione, un nuovo approccio alle esigenze industriali

L'innovazione che emerge in primo piano nella gamma di prodotti Crystal, afferente all'area di offerta denominata Display Computing Solution, consiste nella filosofia costruttiva: si chiama 'Convertible Display System' (CDS), è un sistema che la società ha inventato e brevettato a livello mondiale, e caratterizza tutti i panel PC e monitor della gamma. In sostanza, CDS è una soluzione 'all-in-one' composta da due componenti principali: il modulo sistema e il modulo display.

Questi due elementi separati, una volta combinati assieme grazie a un innesto a baionetta, possono dar luogo, a seconda delle esigenze, a una varietà notevole di configurazioni, grazie alla possibilità per l'utente di abbinare ai moduli sistema, disponibili con caratteristiche hardware differenti (capacità elaborativa della CPU, connettività di I/O, funzionalità e così via), un'ampia serie di display LCD, anch'essi disponibili con diverse caratteristiche in termini di dimensioni, formato (4:3, widescreen), risoluzione, luminosità, tipologia di touchscreen.

Sempre tra le peculiarità da porre in rilievo, è importante sottolineare che la connessione fisica tra modulo sistema e modulo display avviene attraverso un'interfaccia proprietaria, in grado di integrare in un'unica scheda embedded i segnali del display, dello schermo touch e del computer. In aggiunta, grazie a una particolare progettazione meccanica, completamente priva di cavi e fili (cable-less), tale connessione permette di garantire un'affidabile collegamento dei due componenti hardware in un unico corpo, molto compatto (spessore inferiore a 10 cm) e robusto.

La trasformabilità della soluzione CDS è anche data dal fatto che essa supporta due tipi di modulo di sistema: il modulo PC (P1000 Series) basato su processore Intel Atom E3845 quad core a basso consumo, e il modulo monitor (M1000 series), dotato di porte USB, COM, VGA, DVI-D e DisplayPort. Il modulo display (CV-100X series) è compatibile con entrambi. Combinando un modulo display con un modulo PC è possibile ottenere un panel PC (convertible panel PC), mentre unendo un modulo display con un modulo monitor si ottiene un touch monitor (convertible touch monitor). Dunque, la trasformazione di un sistema in un panel PC o in un touch monitor si può eseguire facilmente scegliendo i moduli corretti. I vantaggi di una soluzione modulare come questa, rispetto ai tradizionali sistemi display stand-alone, sono numerosi. Dal punto di vista logistico, proprio la modularità della soluzione rende possibile ridurre gli stock di prodotti in magazzino e migliorare i tempi di consegna della merce. La configurabilità on-demand permette di costruire sistemi application-ready in modo estremamente rapido. La possibilità di aggiornamento e sostituzione dei singoli componenti protegge l'investimento effettuato e fornisce una soluzione con capacità scalabile in rapporto alle diverse esigenze.

Chi è Contradata

Una gamma di prodotti molto ricca (schede e moduli, panel PC e monitor, memorie industriali, embedded box completi) e un ampio ecosistema di partner – fra cui IEI, CONGATEC, ICOP, DFI, TQ, KORENIX, INNODISK – fanno di Contradata una realtà di primo piano in Italia nella distribuzione di soluzioni embedded e PC industriali. Alle attività commerciali e logistiche la società affianca competenze nel supporto design-in (hardware, software, firmware), nell'integrazione di sistemi e nello sviluppo di soluzioni semi-custom e full-custom.

Fig. 2 – Le possibilità di trasformazione delle configurazioni fornite da CDS

La trasformabilità accresce le tipologie e i casi di utilizzo. Infine, la modalità di installazione, di tipo plug-&-play, e il fatto di avere due componenti separati (modulo sistema e modulo display), semplifica molto gli interventi di manutenzione, rispetto ad esempio ai tradizionali panel PC completamente integrati, in cui eseguire operazioni di riparazione può risultare davvero disagevole.
Fra l'altro, sottolinea Contradata, le soluzioni CDS non hanno un costo superiore ai panel PC convenzionali, ma si posizionano su livelli di prezzi analoghi a quelli dei sistemi 'semi-industrial', fornendo livelli di protezione di grado IP65, che mettono lo schermo al riparo da acqua e polvere.
I prodotti Crystal integrano tecnologie display, touch e computing, e sono basati su pannelli con backlight LED di categoria 'industrial grade' ad alta luminosità.
La dotazione di I/O fornisce una estesa connettività, mentre il design ultra-slim amplia le possibilità d'installazione in ambienti diversi (montaggio a muro e così via). Essendo fan-less, i sistemi non hanno parti in movimento, e ciò riduce i rischi di avaria minimizzando i costi di manutenzione. L'assenza di cavi sulle schede accresce la robustezza in caso di shock e vibrazioni.
L'alimentazione estesa da 9 a 48 VDC consente il dispiegamento dei sistemi Crystal in svariati ambienti, mentre i meccanismi di protezione da sovracorrenti e sovratensioni costituiscono un'ulteriore sicurezza. Il formato schermo classico (4:3) si adatta alle applicazioni software più diffuse, mentre quello 'widescreen' (16:9) soddisfa le esigenze di visualizzazione di immagini e video ad alta definizione.
Il touchscreen capacitivo proiettato supporta sia la modalità single-touch, sia quella multi-touch fino a 10 punti, anche con l'uso di guanti.
Al momento in cui scriviamo, il modulo PC è basato solo su Intel Atom, ma presto dovrebbero essere resi disponibili moduli PC equipaggiati con processori Intel Core della quarta generazione (i3, i5, i7), per abilitare applicazioni che richiedono prestazioni particolarmente elevate in termini di grafica HD, contenuti 3D e uso simultaneo di tre display. Sempre il modulo PC possiede un ricco corredo di I/O (Ethernet 10/100/1000; DisplayPort; COM, USB 2.0 e 3.0; Line-out; MIC-in e così via). Anche le comunicazioni wireless sono assicurate, sia a corto raggio, grazie a uno slot Mini PCIe per schede add-on Wi-Fi (802.11), sia a livello geografico su reti cellulari, attraverso uno slot per SIM card, e uno MiniPCIe per schede add-on HSUPA.
Ancora, il particolare tipo di design facilita in modo notevole l'accesso ai dispositivi di storage (HDD/SSD; CFAST; SIM card), velocizzando l'ingresso nel modulo per arrivare ai dati o per agevolare interventi di sostituzione o manutenzione. La flessibilità di abbinamento dei componenti abilita con facilità la realizzazione di applicazioni multi-display. La gamma di sistemi Crystal si declina in molti ambiti di utilizzo tra cui automazione industriale, sicurezza e sorveglianza, trasporti, digital signage e building automation.

Fig. 3 – Il sistema CDS facilita le attività di manutenzione

Fig. 4 – La linea di prodotti Crystal comprende un'ampia gamma di display

PC industriali, tre linee chiave

All'area di offerta Fanless Computing Solution appartengono i sistemi di computing industriali della linea Diamond, suddivisa a sua volta in tre categorie di prodotti. La prima è la serie Diamond C (Compact) e include macchine entry level con processore Intel Atom (Pineview o Bay Trail), ultracompatte e a basso consumo, con prestazioni efficienti, e adatte ad applicazioni embedded in spazi limitati. A una categoria intermedia appartengono invece i sistemi della serie Diamond E (Efficient), sempre basati su Atom ma ricchi di I/O, dunque maggiormente espandibili (PCI, PCIe) e dotati di una flessibilità che li rende adatti a una vasta tipologia di applicazioni industriali.

La partnership con innodisk

Con l'obiettivo di indirizzare i propri clienti verso le soluzioni di memorizzazione dati più affidabili per le diverse applicazioni, mantenendo prezzi convenienti, Contradata ha scelto per lo storage la collaborazione con innodisk, produttore di dispositivi di memorie flash con alte prestazioni e affidabilità per applicazioni industriali e sistemi embedded. I sistemi Contradata sono configurati con questi supporti di storage, scegliendo di volta in volta i dispositivi (SSD, SATADOM, SATA Slim, mSATA, CompactFlash e così via) con i requisiti più adatti alle specifiche della singola applicazione.

Infine, la serie Diamond S (Superior) raccoglie le macchine 'high end' con processori Intel Core di quarta generazione (i3/i5/i7) a elevata potenza di elaborazione, funzionalità multi-tasking e possibilità di espansione ancora più marcate, per soddisfare le applicazioni più critiche.
Oltre ai concetti costruttivi 'cable-less' e soprattutto 'fanless'- quindi niente parti in movimento, assenza di rumore e MTBF esteso fino a 100 mila ore – vi sono funzionalità specifiche da porre in rilievo, ad esempio, la regolazione dell'accensione per applicazioni veicolari (power ignition for vehicle), la funzionalità RAID per attività di backup e recovery; opzionali: il Power over Ethernet (PoE) e il supporto multi-LAN Gigabit, per applicazioni di networking. In aggiunta, la scelta di realizzare il case di contenimento con un corpo unico, e non con diverse parti assemblate, migliora la dissipazione del calore, oltre che la robustezza a shock e vibrazioni, e la protezione contro polvere e acqua.
Le temperature operative supportate in alcuni modelli vanno da -20 a +70 °C, per l'adattamento ad ambienti molto severi. I componenti elettronici sono di livello 'industrial grade'. In aggiunta, i prodotti Diamond supportano un'ampia gamma di tensioni d'ingresso (9-48 VDC) per essere alimentati in modo sicuro in molte condizioni.
Non mancano poi i meccanismi di protezione contro l'inversione di polarità, le sovratensioni, le sovracorrenti, e per la protezione ESD (electrostatic discharge) contro le scariche elettrostatiche. Infine, sulle macchine Diamond, la compattezza non sembra penalizzare l'espandibilità, grazie agli slot Mini-PCIe e allo 'universal I/O bracket', un sistema di espansione che permette l'aggiunta di schede di I/O e di comunicazione wireless.

Fig. 5 - La famiglia di embedded box Diamond

Fig. 6 - La facilità d'accesso alle periferiche garantisce praticità e manutenibilità

Cincoze, il posizionamento

Cincoze si colloca sul mercato come fornitore di sistemi nel comparto dell'industrial computing, progettando, costruendo e commercializzando prodotti altamente ingegnerizzati e innovativi. L'azienda si concentra sui processi chiave di realizzazione di una soluzione completa, dallo studio di fattibilità, alla progettazione, alla fase di verifica, alla produzione, fino ai servizi che puntano ad assicurare un lungo ciclo di vita dei prodotti.
Le sue competenze spaziano dalla progettazione e ottimizzazione dell'elettronica e dei circuiti, per il superamento dei test con i requisiti più stringenti; alla progettazione meccanica, in linea con le necessità di safety e affidabilità delle applicazioni embedded; alla progettazione termica – finalizzata ad aiutare i clienti a superare i problemi di dissipazione del calore – che si avvale di strumenti di simulazione e attrezzature di test, per collaudare le prestazioni di ogni progetto meccanico.
Il processo di produzione include la realizzazione delle PCB e degli chassis di alluminio. Le fabbriche di assemblaggio, localizzate in Taiwan, seguono piani di manufacturing rigorosi, per rispettare gli obiettivi in termini di numero di pezzi e tempi di consegna. Tutti i prodotti sono sottoposti a severi test di verifica.

La combinazione M2M e IoT spinge il business

Spirale ascendente nell'adozione di tecnologie M2M dall'avvento dell'Internet of Things

Francesca Prandi

Alexander Damisch, senior director of IoT Solutions, Wind River
"Ci sono più di un miliardo di device M2M all'opera nel mondo come sensori, smart meter, sistemi di controllo industriale, sistemi di monitoraggio medicali mobili, di videosorveglianza, soluzioni automotive e telematiche, edifici intelligenti e così via. Le sole connessioni wireless M2M, stando a un report Berg Insight sono cresciute del 37% lo scorso anno, raggiungendo il numero di 108 milioni. Tutti segnali dell'enorme opportunità di crescita che l'Internet delle Cose (IoT) offre al M2M. L'utilizzo dell'IoT è favorito da vari aspetti. Una domanda molto elevata di Big Data in tempo reale al fine di contribuire a decisioni di business veloci e più intelligenti. La necessità di ridurre i costi del lavoro delegando ai sistemi, ora più intelligenti, lo svolgimento di compiti che richiedono consapevolezza della situazione presente. I sistemi intelligenti possono diventare una sorta di rampa di lancio verso il cloud e il suo potenziale. Altri aspetti di contesto che favoriscono l'IoT sono le tematiche ecologiche (i compiti svolti rapidamente e in modo intelligente dalle macchine riducono ad esempio il consumo energetico) e la cultura della gratificazione istantanea, per cui clienti e fornitori desiderano tutte le risposte in modo quasi immediato.

Alexander Damisch, senior director of IoT Solutions, Wind River

> **"I sistemi intelligenti possono diventare una sorta di rampa di lancio verso il cloud e il suo potenziale"**
>
> **Alexander Damisch**

Per lo sviluppo dell'IoT Wind River si concentra su tre tematiche chiave: connettività, gestibilità, sicurezza. A queste priorità rispondiamo attraverso la Wind River Intelligent Device Platform, un ambiente di sviluppo software completo che consente di passare subito allo sviluppo IoT. Creando un approccio standardizzato, tutte le problematiche risultanti dal fare da sé (DIY) sono eliminate e le companies possono così concentrarsi sulle proprie specificità accelerando così il time-to-market." (*)

Il barometro del M2M di Vodafone è orientato al bello

Attraverso una ricerca di mercato a cadenza annuale, Vodafone tiene monitorata l'attitudine delle aziende verso il M2M, le decisioni di utilizzo e i progetti per il futuro. L'indagine, 'The M2M Adoption Barometer 2014', condotta nella primavera di quest'anno da Machina Research, ha coinvolto circa 600 aziende delle diverse aree geoeconomiche mondiali ed è stata svolta seguendo varie metodologie (quantitative e qualitative) per integrare poi i dati ottenuti. I paesi rappresentati nel 2014 sono Australia, Brasile, Cina, Germania, India, Italia, Giappone, Paesi

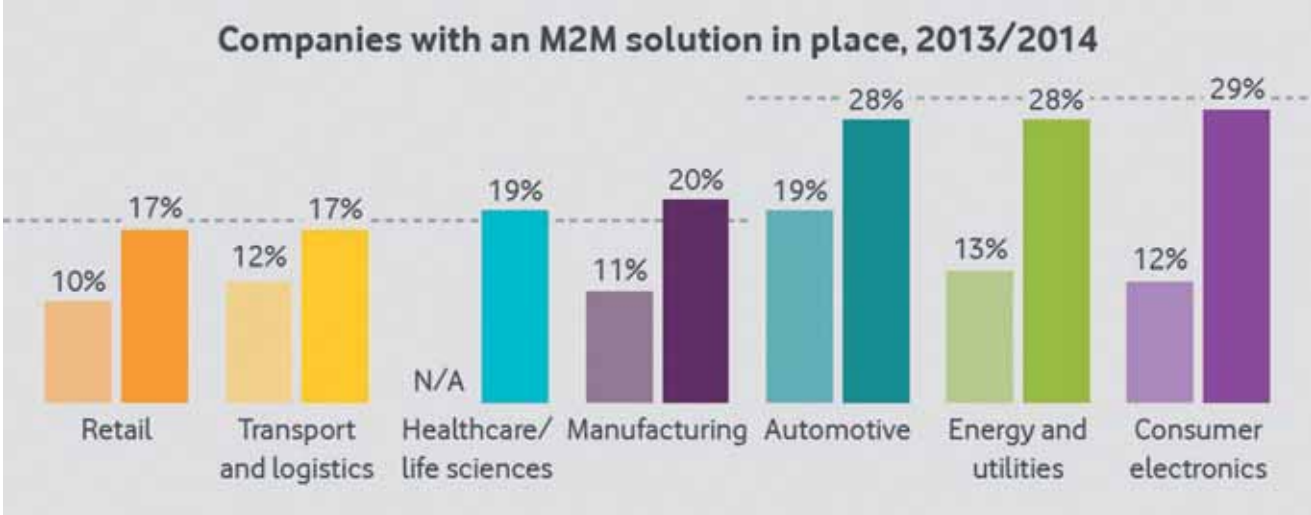


Fig. 1 – Crescita percentuale di adozione di una soluzione di M2M sul totale delle aziende appartenenti allo stesso settore industriale (Fonte Vodafone)

Bassi, Sud Africa, Corea del Sud, Spagna, Turchia, UK e Usa. Il primo dato che emerge è che il 22% delle aziende intervistate dispone di almeno una soluzione di M2M e il 55% progetta di realizzarne una entro due anni.
Dal confronto con la stessa indagine compiuta l'anno precedente presso gli stessi interlocutori (altri si sono aggiunti nel Barometer 2014) emerge come l'adozione continui spedita. Si veda a tal riguardo la figura 1, che rappresenta la crescita della percentuale di adozione sul totale delle aziende appartenenti allo stesso settore industriale. Le previsioni degli intervistati sul livello di adozione entro il 2016, rappresentate in figura 2, mostrano un trend crescente, più o meno marcato, per tutti i rami industriali.
Le soluzioni IoT richieste dai vari settori sono infinite ed estremamente varie e tuttavia vi sono tre temi comuni che le attraversano: la gestione delle flotte, molto richiesta nel retail, manufacturing, automotive e

"Il termine M2M implica il collegamento di device e il trasferimento dei dati."

"Il M2M è come un impianto su cui si inserisce l'Internet delle Cose (IoT)."

Matt Hatton

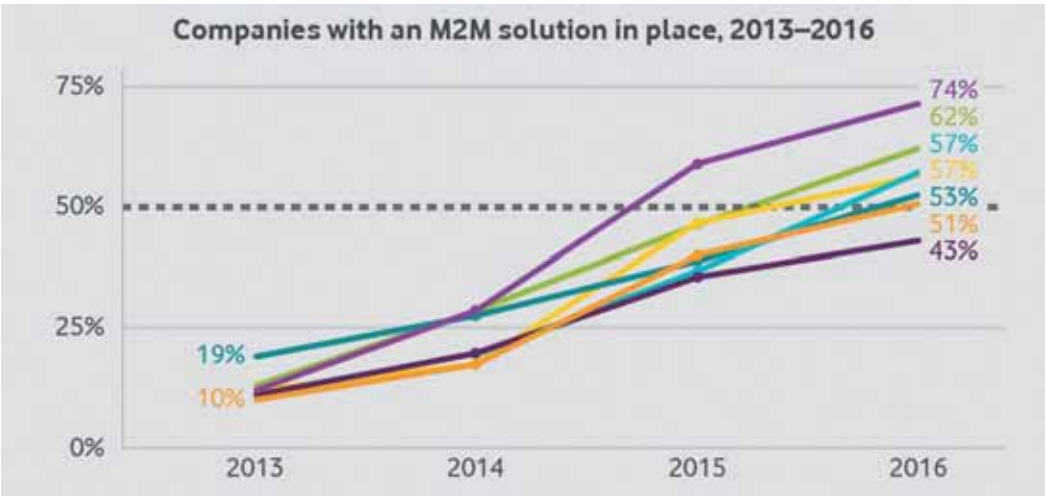


Fig. 2 – Livello di adozione di una soluzione di M2M entro il 2016 (Fonte Vodafone)

Matt Hatton, direttore di Machina Research

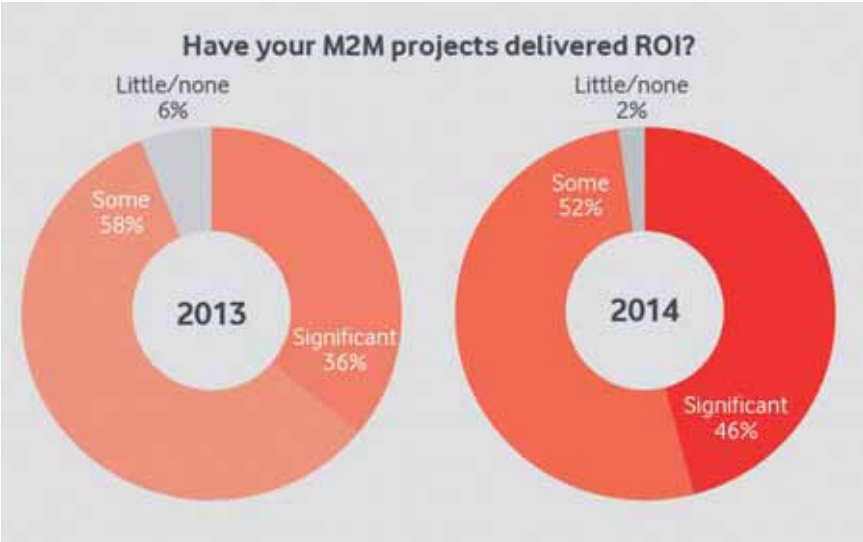


Fig. 3 – Livello del ROI del M2M (Fonte Vodafone)

trasport; il tracking degli assets, soprattutto quelli di valore (con la riduzione del costo delle soluzioni si estenderà anche ai beni meno costosi); il monitoraggio delle persone: per la sicurezza nel manufacturing, per lavoratori in ambienti isolati e/o pericolosi nell'healthcare, trasporti, energy e utilities. "Attualmente il M2M viene abbracciato prevalentemente per obiettivi interni all'impresa, ovvero per rendere i processi di business più efficienti –afferma Matt Hatton di Machina Research. La prossima ondata di adozione, riguarderà anche i modelli di business e i prodotti, modificandoli. Oggi c'è ancora un po' di esitazione, ma le pressioni competitive alla fine imporranno l'adozione del M2M." La ricerca conferma che il ROI del M2M è elevato e addirittura si materializza prima delle attese, tanto che ben il 98% delle aziende dichiara un ROI positivo se non addirittura significativo, come si osserva nella figura 3. Rispetto al Barometer 2013 "l'idea di utilizzare il M2M per accrescere il proprio vantaggio competitivo ha acquistato molto credito" e questo farà da volano sulle decisioni di investimento.

> **"In a lot of cases the M2M solutions are now becoming more effective thanks to the IoT"**
>
> **Dirk Finstel**

Un tema sempre caldo in ogni stagione di innovazioni IT è quello della sicurezza. La ricerca dimostra come le aziende considerino questa come una delle varie sfide da affrontare; sfida che tuttavia non è in grado di bloccare il trend positivo di adozione. Infatti solo il 12% degli intervistati vede nella sicurezza l'aspetto di maggiore preoccupazione. Molto interessanti sono le previsioni avanzate dall'analista di Machina Research.

Il M2M verrà spinto e a sua volta spingerà un approccio big data e analytics affinché dalla grande massa di dati raccolti possano emergere elementi utili per una strategia. Già oggi il 75% degli intervistati dichiara di utilizzare analytics e l'88% ritiene di arrivarci entro tre anni.

Le tecnologie 4G renderanno funzionali ed efficienti molte nuove applicazioni, inclusa la security basata su video, i servizi di informazione dentro il veicolo, soluzioni per l'assistenza al living e ai malati e così via. Il manifatturiero e l'automotive faranno molto meglio di quelle che sono le aspettative rilevate dalla ricerca, che indica l'elettronica di consumo come settore dominante nell'utilizzo del M2M. Nel manifatturiero, infatti, sta crescendo la comprensione del valore del M2M e nell'automotive saranno gli stessi automobilisti a richiedere servizi a bordo veicolo, con effetti persino sull'aftermarket.

Cresce l'intelligenza richiesta al M2M

Intervista a Dirk Finstel, Ceo EMEA di Adlink Technology

Iniziata l'epoca dell'Internet delle Cose quali evoluzioni riscontrate nel mercato M2M?

"In tutti i mercati finali osserviamo la tendenza a migliorare la gestione del controllo a distanza e dei servizi di previsione delle manutenzioni necessarie a evitare il fermo macchina. In questo modo le aziende riescono a ridurre il costo totale di ownership, a un aumentare le vendite e a ottenere una maggiore soddisfazione del cliente.

Questi obiettivi, resi possibili dal M2M, nel caso di Adlink sono raggiunti ancora meglio grazie alla disponibilità del cloud che viene offerto embedded nelle schede e nei sistemi. Lo abbiamo chiamato SEMA, Smart Embedded Management Agent, ed è presente in tutte le nostre ultime schede e sistemi embedded consentendo il trasferimento dei dati richiesti nel cloud con una comunicazione bi-direzionale, che abilita la configurazione del sistema

Dirk Finstel, Ceo EMEA di Adlink Technology

e il management da remoto. Attraverso le tecnologie IoT e il cloud anche le applicazioni per il cliente finale possono utilizzare questo canale di comunicazione e in tal modo gli ingegneri degli OEM si trovano di fronte una base tecnologica completa che ne aumenta l'affidabilità; possono essere manutenute e controllate in modo più efficiente proprio grazie ai servizi cloud based.
Riteniamo che questo approccio al M2M orientato al futuro e la nostra strategia IoT, con un servizio cloud tagliato sui device embedded che produciamo, siano davvero unici nel mercato e che tutto questo ci consentirà di confermare nei prossimi anni una crescita dei ricavi a due cifre nonché un incremento dei margini."

Quali settori finali sono particolarmente coinvolti in queste evoluzioni?
"La connettività a banda larga attraverso Internet arricchisce le applicazioni degli OEM in diversi settori industriali come l'automazione, i trasporti, l'energia e l'infotainment. Nell'ambito della manutenzione, in generale, possiamo immaginare una situazione nella quale il tecnico che interviene sulla macchina ricava le istruzioni per la riparazione sia dalle informazioni rese disponibili in loco dalla macchina stessa sia da un supervisore collegato in videoconferenza.
Nel settore industrial, dove i prodotti devono avere un ciclo di vita lungo, la manutenzione è un tema fondamentale. Nei trasporti si possono tagliare i costi con applicazioni di logistica intelligente più evolute. Nel settore dell'energia si moltiplicano i device connessi in una smart grid che deve essere gestita in modo sempre più intelligente e ciò porta a implementare nodi M2M più evoluti. Nell'infotainment, con i grandi numeri di device distribuiti nel vending, nel retail, nel ticketing, nel gaming e nel digital signage, il M2M sta diventando l'unica via attraverso la quale aggiornare il software, riducendo così drasticamente le precedenti manutenzioni sul campo e il content delivery."

Quali sono i temi caldi per un fornitore di piattaforme M2M che utilizzano Internet?
"Per supportare i propri clienti OEM in modo più efficace, i vendor di embedded computing devono fornire anche il middleware appropriato, nel nostro caso SEMA, e il corrispondente cloud M2M. Senza un cloud appropriato con una connettività affidabile e sicura per quanto riguarda l'accesso via internet, i malware e gli attacchi esterni, i clienti sono sostanzialmente nei guai. Tutti i problemi di sicurezza devono essere risolti a partire dal livello device in avanti. Come Adlink abbiamo investito non solo nell'implementazione delle tecnologie standard, come ad esempio AES encryption, ma anche nel nostro hardware-based encription engine. A questo punto l'attacco criminale a tecnologie proprietarie richiede uno sforzo estremamente elevato e per nulla remunerativo. È sicuramente più conveniente aggredire soluzioni standard che generano milioni di bits di informazioni utilizzabili. La connettività deve essere estremamente stabile e flessibile con un'ampiezza di banda scalabile. Come protocollo di comunicazione, crackato SSL, oggi occorre almeno TLS 1.2. Un tema caldo è anche la stabilità del cloud. I clienti embedded e M2M non possono affidarsi a offerte commerciali. Questi OEM devono offrire ai loro clienti un cloud embedded che sia disponibile nel lungo periodo, che sia stabile e validato per applicazioni che comprendano anche un 'frozen' software status (nel caso di interruzione della connettività, i dati già trasferiti vengono congelati per ridurre i costi di trasferimento di elevati volumi di dati)."

Quali nuove caratteristiche emergono in ordine all'hardware?
"Le piattaforme ARM rappresentano una buona scelta per una raccolta dati decentralizzata e per soluzioni M2M deeply embedded. Anche le piattaforme Intel Atom SoCs sono adatte per un'ampia gamma di appliances M2M. Avranno grandi possibilità i prossimi processori Intel Quark, che impatteranno sicuramente sul mercato dei piccoli dispositivi M2M. Per quanto riguarda le interfacce per connettere i sensori ai device edge e ai sistemi, prevarranno gli standard wireless WLAN, Zigbee e Bluetooth perché minimizzano il cablaggio e riducono i costi e i tempi di implementazione oltre a consentire dei semplici upgrades del macchinario esistente con maggiore intelligenza. Questi sono i trend della domanda di un'automazione sempre più intelligente."

Cresce l'impulso nella domanda di soluzioni per automotive, telematica e servizi a valore nell'IoT

Intervista a Tony Spizzichino, senior sales director Italy & South Eastern Europe di Telit

Tony Spizzichino, senior sales director Italy & South Eastern Europe di Telit

Quali maggiori trend osservate nei settori del mercato M2M nell'epoca dell'Internet delle Cose?
"Gli ambiti applicativi che più di altri alimentano la curva di sviluppo dell'Internet delle Cose, ampliando le opportunità nel segmento dell'M2M, e che più di altri rappresentano

interessanti opportunità di mercato sono lo healthcare, la domotica, l'automotive e lo smart metering. Uno dei trend emergenti nell'industria delle soluzioni M2M è sicuramente quello dei prodotti location-based miniaturizzati per i wearable device. Grandi aziende con importanti capacità di investimento e/o early adopter sono i primi a cimentarsi con la sfida del passaggio all'IoT. Negli ultimi anni abbiamo registrato una crescita sostenuta e costante a doppia cifra della domanda di soluzioni e ritengo che questo trend continuerà nel tempo grazie alle potenzialità dell'intero mercato M2M.
Prevediamo un deciso impulso nella domanda di soluzioni per automotive e telematica nonché di servizi a valore nella IoT (M2Mair e Cloud). Ci aspettiamo anche una crescita nelle vendite di prodotti cellulari 3G e 4G nonché di moduli di posizionamento e short range per applicazioni nel segmento dell'Energy (tecnologia W-Mbus destinato a contatori intelligenti) e domotica."

"Prevediamo un deciso impulso nella domanda di soluzioni per automotive e telematica nonché di servizi a valore nella IoT".

Tony Spizzichino

Quali settori applicativi saranno trainanti e quali altri potrebbero affacciarsi sul mercato con buone prospettive di business?
"Telematica (automotive e after market), smart metering, domotica, sicurezza, sanità, pagamenti elettronici e smart city saranno i settori trainanti. Una delle principali aree di crescita in Europa è rappresentata dal mercato automotive. Infatti, oltre all'evoluzione degli impianti di infotainment e navigazione messa a punto dalle case automobilistiche, la spinta al segmento viene anche dalla regolamentazione della Commissione europea che prevede che tutte le nuove auto debbano avere entro il 2015 un sistema di emergenza automatico a bordo dei veicoli, denominato eCall, che richiede una connettività wireless e location-based."

Quali sono i temi caldi per un fornitore di piattaforme M2M che utilizzano Internet?
"La sfida principale risiede nel non completamento e in alcuni casi nella mancanza totale di uno standard definito. Ciò impatta sulla selezione delle caratteristiche tecniche delle soluzioni da adottare nonché del formato e/o protocolli di comunicazione.
La connettività deve essere adeguata all'esigenza di scambio dati dell'applicazione.
Ad oggi esistono molte soluzioni tecnologiche che già offrono sufficiente copertura. Nonostante ciò ci aspettiamo continui miglioramenti nelle performance sulla falsa riga dell'esperienza che abbiamo già compiuto negli ultimi 20 anni sul segmento cellulare. Avranno un grande impatto anche soluzioni innovative per la riduzione dei consumi e nell'energy harvesting, abilitando sensori/attuatori che non necessitano di alimentazione esterna o sostituzione di batterie.
Diverso è il discorso della sicurezza, che nell'IoT risulta particolarmente importante: infatti, anche se si parte dalla grande esperienza di Internet, problemi di hackeraggio in questo ambito potrebbero causare effetti drammatici sulla società."

Quali nuove caratteristiche tecnologiche dei componenti hardware e software soddisfano oggi al meglio i requisiti delle soluzioni M2M richiesti dal mercato?
"L'hardware deve essere in grado di incrementare le capacità dei dispositivi, aggiungendo funzionalità, connettività, caratteristiche di safety e security, e riducendo al contempo i costi. Le applicazioni devono essere basate su piattaforme integrate che consentono di rilasciare sul mercato prodotti molto avanzati in tempi ridotti e costi contenuti, ottenendo un aumento di affidabilità e qualità dovuto alla riduzione del numero di componenti necessari."

Quali evoluzioni osservate nella struttura della supply chain M2M?
"La rapida diffusione delle soluzioni M2M a un'infinità di settori applicativi offre ai grandi player della supply chain l'opportunità di proporsi come interlocutore unico per tutti gli aspetti attinenti la soluzione: dall'hardware, al software, alla connettività e a tutti i servizi connessi.
Ad altri livelli della supply chain si sviluppano alleanze e nascono nuove società che hanno l'obiettivo di unificare alcuni step della supply chain stessa. Telit si definisce 'One Shop' infatti, oltre a disporre di un ampio portafoglio M2M in tecnologie cellulari, short range e di posizionamento, insieme ai servizi m2mAIR per la connettività mobile e cloud, offre anche un supporto globale e logistico in grado di rispondere a ogni bisogno o richiesta di clienti grandi e piccoli."

Nota
(*) Osservazioni dal White Paper di Wind River "Smarter Ways to Use the Internet of Things"

Analizzatore di rete vettoriale integrato in un unico slot PXI

La nuova serie M937xA di Keysight Technologies è formata da VNA in grado di coprire la gamma di frequenza da 300 kHz a 26.5 GHz, che si distingue per le sue caratteristiche in termini di velocità, stabilità e range dinamico

Maurizio Di Paolo Emilio

La crescente richiesta di sistemi di analisi di rete vettoriale con un elevato numero di porte (2,4,8 e così via) e la necessità di ridurre le dimensioni con maggior funzionalità, hanno ispirato Keysight a sviluppare l'analizzatore di rete vettoriale (Vector Network Analyzer, VNA) M937XA Serie PXIe. La serie è utilizzata per misurazioni accurate, consentendo la caratterizzazione simultanea di molti dispositivi a due o multi porte, utilizzando un unico chassis PXI. Le aziende che si occupano dello sviluppo di sistemi decidono di investire in misura sempre maggiore in attrezzature hardware di misura modulare, sia esse completamente modulari o ibride.

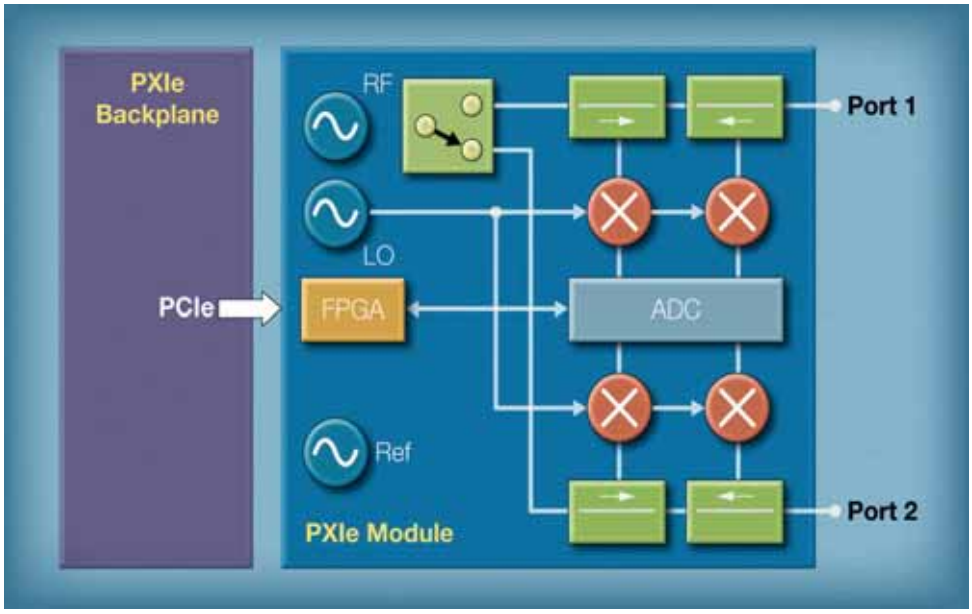


Fig. 1 – Schema a blocchi dell' M937xA

Anche se non porterà a una riduzione dei costi, molti si aspettano che a lungo termine possa influenzare sui costi di sistema in maniera positiva.

Recentemente sono emersi tre temi principali in ambito del test industriale:

- la necessità di testare dispositivi molto complessi in molto meno tempo senza sacrificare la precisione;
- la necessità di testare più dispositivi in una sola stazione di prova;
- la necessità di ridurre le dimensioni delle stazioni di prova utilizzati per testare diversi dispositivi complessi.

Il successo di un prodotto dipende, quindi, dalla capacità di soddisfare queste esigenze, mentre bisogna far fronte alla crescente complessità di wafer di silicio, dispositivi wireless, sistemi radar avanzati, e altro ancora, che continuano a confezionare più funzionalità in meno spazio.

Fig. 2 – M9370A Serie PXIe VNAs two-port

Questi requisiti hanno ispirato Keysight nel creare un importante sistema di analisi vettoriale delle reti: M937xA Serie PXIe VNA (Fig. 1). Si tratta di dispositivi a due porte che, integrate in un solo slot, svolgono misurazioni accurate e veloci; inoltre, riducono il costo del test consentendo la caratterizzazione simultanea di molti dispositivi Multi-port con un unico chassis PXI (Fig. 2). Questi analizzatori coprono un range di frequenze cha vanno da 300 kHz fino a 26,5 GHz (sei modelli disponibili, Fig. 3) permettendo ai progettisti la copertura di frequenza necessaria; offrono, inoltre, migliori prestazioni sulle specifiche fondamentali quali la velocità, il rumore, la stabilità e la gamma dinamica.

La serie M937xA two-port

Nel corso degli anni Keysight ha migliorato la scelta dei suoi VNA in strumentazione da banco, con l'aumento del numero di porte per essere utilizzati simultaneamente. Soluzioni che richiedono più di otto porte spesso diventano ingombranti in termini di dimensioni, cablaggio e consumo energetico.
Il PXI VNA della serie M937xA è un dispositivo di 95 x 178 x 19 mm, all'interno del quale (uno slot) vengono fornite le seguenti caratteristiche:

- Sweep speed: da 28 a 33 msec attraverso 401 punti.
- Gamma dinamica: maggiore di 116 dB a 9 GHz e maggiore di 98 dB a 20 GHz.
- Trace noise: minore di 0,001 dB.
- Stabilità (tipica): 0,005 dB/°C.

L'analizzatore di rete vettoriale M937xA PXIe consente in particolare le misure dei parametri S e la distorsione armonica ad alta velocità fino a 27 GHz. Parametri S sono riferiti alla matrice di scattering, un costrutto matematico che quantifica come l'energia RF si propaghi attraverso una rete multi-porta. La distorsione armonica, invece, esprime l'alterazione di un segnale nelle sue forme di frequenza e fase, generando delle nuove frequenze che non erano presenti nel segnale iniziale e che vengono considerate come rumore. Il THD (Total Armonic Distorsion) è una grandezza di misura che esprime la qualità di un dispositivo.
Il PXI VNA utilizza la scienza e la tecnologia di calibrazione dei popolari analizzatori di rete Keysight PNA: through-reflection-line (TRL), short-open-load-through (SOLT) e tutte le altre procedure specializzate. Inoltre, offre calibrazioni guidate e piena capacità di calibrazione multi-porta, ed è compatibile con i kit di calibrazione meccanici così come i kit di taratura elettronica (ECal). I modelli PXI forniscono anche un'interfaccia utente grafica che condivide il familiare "look and feel" della famiglia PNA e facilita la transizione verso le PXI (Fig. 4).
Tutte queste funzionalità possono essere configurate per soddisfare la gamma di scenari descritti nell'introduzione: uno slot VNA per un singolo chassis di tester multifunzione, fino a otto VNA a due porte in un singolo chassis, o moduli in combinazione flessibile di analizzatori multi-porta in un unico chassis (Fig. 5).
La serie M937xA è disponibile nelle seguenti varianti:

M9370A, 300 kHz - 4 GHz,
M9371A, 300 kHz - 6.5 GHz,
M9372A, 300 kHz - 9 GHz,
M9373A, 300 kHz - 14 GHz,
M9374A, 300 kHz - 20 GHz,
M9375A, 300 kHz - 26.5 GHz.

Fig. 3 – M937xA, sei modelli disponibili per un vasto range di frequenze

Varie funzionalità di misura sono disponibili attraverso una gamma di opzioni software. Capacità opzionali includono l'analisi nel dominio del tempo, calibrazione N-port e capacità avanzate di simulazione.
I vari fattori di forma e flessibilità del PXI VNA, soddisfano le esigenze emergenti nel settore aerospaziale, difesa, comunicazioni wireless, dispositivi elettronici, e altro ancora.

Tecnologia PXI/PXIe

PCI eXtensions for Instrumentation (PXI) è una delle diverse piattaforme di strumentazione di elettronica modulare maggiormente utilizzate per la costruzione di apparecchiature elettroniche di prova e sistemi di automazione.
PXI è basata su bus di computer standard di settore e aggiunge bus di sincronizzazione specializzati e funzioni software (Fig. 6).
PXI supporta due fattori di forma, 3U e 6U: la forma 3U ha due connettori di interfaccia, J1 (32 bit) e J2 (64 bit); la forma 6U, invece, può trasportare fino a tre connettori supplementari per una futura espansione della specifica PXI. Diverse caratteristiche tecniche del PXI permettono di eseguire prove e misure più rapide. In virtù di sfruttare la tecnologia del computer, PXI si avvale dei più recenti progressi nei processori riducendo i tempi di post-elaborazione. Il bus backplane PXIe sfrutta anche la tecnologia PC PCI Express Gen2, aumentando notevolmente il throughput e riducendo la latenza. Inoltre, i sistemi PXI Keysight includono un'architettura integrata semplificata con accesso diretto alla memoria.

Applicazioni e software

La serie M937xA è ideale per test in ambito aerospaziale/manutenzione, componenti wireless e test di produzione specifici. Il PXI VNA può essere integrato con altri moduli di test e di automazione sia in un PXIe sia Hybrid. Keysight IO Libraries Suite offre un rapido e facile collegamento sia a strumenti tradizionali sia modulari; permette di visualizzare tutti i moduli del sistema, siano essi PXI o PXIe. È possibile visualizzare le informazioni riguardanti il software installato direttamente da Expert Connection Keysight (KCE); KCE offre un modo semplice e veloce per trovare il driver corretto al sistema. M937xA PXI VNA è fornito con un portafoglio completo di driver, documentazione, esempi e strumenti software per aiutare a sviluppare rapidamente sistemi di test con la piattaforma software di scelta. Il modulo viene fornito con driver IVI-COM, IVI-C, LabVIEW e MATLAB che lavorano negli ambienti più popolari di sviluppo tra cui, LabWindows / CVI di National Instruments, Microsoft C/C ++, C # e VB.NET (oltre a LabVIEW e Matlab).

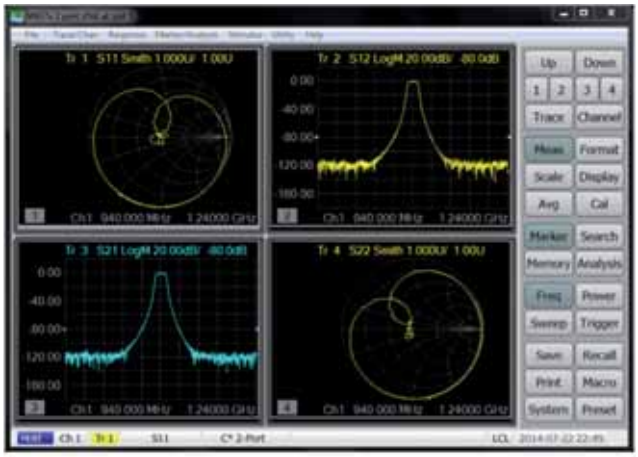


Fig. 4 – Interfaccia utente della PXI VNA

Fig. 5 – Configurazione multi-port con 8 PXI VNA two-port in un singolo chassis

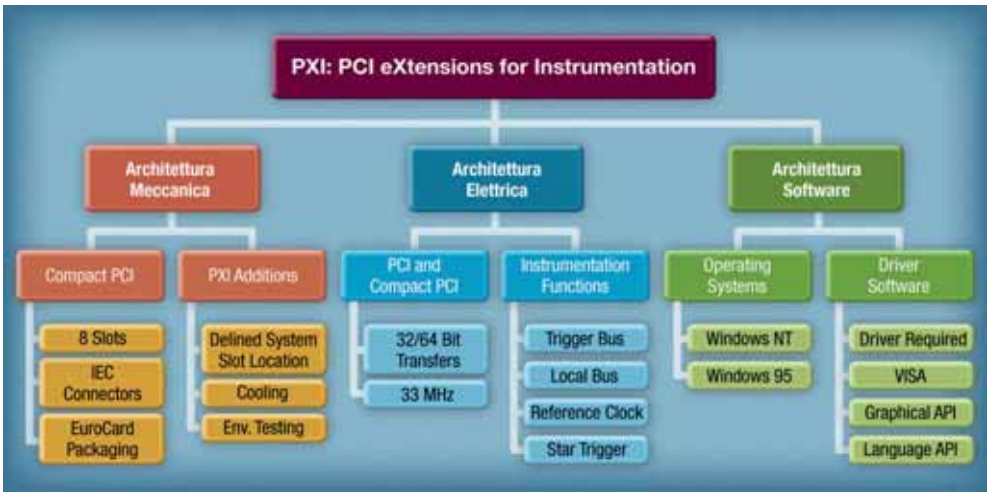


Fig. 6 – PCI eXtensions for Instrumentation (PXI)

Robustezza militare con componenti commerciali

I componenti rugged hanno specifiche in grado di soddisfare le applicazioni militari e in più offrono il vantaggio del minor costo e il valore aggiunto di una disponibilità di prodotti molto più ampia

Lucio Pellizzari

È noto che l'industria delle schede embedded sia da molti anni trainata dall'evolvere delle tecnologie sviluppate nei laboratori dei costruttori che lavorano prevalentemente se non esclusivamente per il dipartimento della difesa (DoD) statunitense. Quasi tutte le normative riguardanti la robustezza dei materiali e l'affidabilità dei sistemi che circolano oggi sono nate al momento di progettare nuovi sistemi militari o aerospaziali dalle prestazioni elevate tanto quanto i costi, al punto da dover passare persino un certo periodo di tempo coperte da segreto. D'altra parte, la domanda di sistemi e componenti robusti è cresciuta molto di più al di fuori del settore militare e abbraccia oggi svariati altri settori industriali come l'automotive, il medicale, l'energia e l'edilizia, ragion per cui si sono da qualche anno imposte fra i leader nello sviluppo e nella fabbricazione dei prodotti embedded robusti, o rugged, anche numerosissime altre imprese americane, asiatiche ed europee. È evidente che la differenza sostanziale fra queste ultime e quelle che si dedicano solamente al settore militare USA sta nei prezzi, che fortunatamente scendono parecchio sia perché i costruttori sono liberi dal vincolo di rispettare i requisiti oltremodo severi delle normative militari, sia perché si trovano in un regime di concorrenza notevolmente più grande e strutturalmente più aperto.
Di conseguenza, negli ultimi tempi si osserva un'inedita inversione di tendenza che vede i costruttori di sistemi militari USA interessarsi dei prodotti fabbricati per altri usi e non viceversa come è stato per molti anni. Oltre al prezzo notevolmente più basso, i prodotti commercial-off-the-shelf, o COTS, che significa commercializzati e liberamente disponibili sul mercato, hanno fra i vantaggi una robustezza elevata quanto quella militare e in molti casi superiore, un'ampia scelta di versioni e dotazioni e, assolutamente da non sottovalutare, l'assistenza da parte di team di supporto con esperienza su copiose casistiche di applicazioni. Si spiega, quindi, perché i blasonati progettisti dei laboratori militari si trovino sempre più spesso a risolvere i guai che incontrano nel loro lavoro di sviluppo ricorrendo a prodotti commerciali. Per questo motivo è nata la

Fig. 1 – Amphenol produce connettori 38999 con specifiche più severe rispetto a quelle militari e li offre in numerosi modelli per un'ampia varietà di applicazioni COTS

sigla COTS+ che definisce i dispositivi commerciali che hanno caratteristiche di robustezza adeguate per le applicazioni militari e aerospaziali.

Questione di standard

Gli standard militari USA sono ancora predominanti in gran parte dei prodotti rugged e conservano la codifica che il DoD impone caratterizzata dalla sigla MIL-STD o "military standard", che talvolta si trova nella forma MIL-SPEC oppure MilSpecs o "military specification". A completare le norme militari si trovano le MIL-PRF o "performance specification", che prescrivono le prestazioni minime garantite per ciascuna funzionalità operativa da svolgere con un determinato prodotto e le MIL-DTL, o "detail specification", che prescrivono i parametri descrittivi dei materiali e delle tecniche di fabbricazione che bisogna utilizzare affinché i dispositivi e i componenti possano essere impiegati nelle applicazioni militari e aerospaziali.
La più celebre è la normativa MIL-STD-883 che definisce i metodi di test sui sistemi e sui circuiti microelettronici destinati all'uso militare e aerospaziale. In pratica, prescrive una serie lunghissima di test che devono essere eseguiti e certificati affinché un dispositivo o un sistema elettronico soddisfi i requisiti di affidabilità e immunità prescritti per le condizioni ambientali militari, notevolmente più severi rispetto a quelli normalmente previsti per i dispositivi industriali. C'è poi il MIL-STD-202 che prescrive i test sui componenti e sui sottosistemi elettronici sottoposti alle condizioni di stress più critiche come l'85% di umidità, le temperature oltre 100 °C e cose simili. Fra i MIL-DTL, il 38999 descrive le caratteristiche dei connettori in termini elettrici, meccanici e termici, con tolleranza in temperatura che può estendersi perfino da -65 a +200 °C per talune applicazioni. Le norme MIL-PRF 55365 e 55681 descrivono le caratteristiche dei condensatori di tantalio e di quelli ceramici espressamente progettati per le applicazioni rugged. Infine, gli standard AEC-Q101, Q200 e Q003 sono nati in seno all'Automotive Electronics Council per normare i test sulla qualità dei componenti elettronici utilizzati nell'industria automotive in termini di immunità alle alte temperature, alle vibrazioni, agli urti e all'inquinamento tipico degli ambienti che ospitano i motori nei mezzi di trasporto di qualsiasi tipo. La differenza è che il Q101 si rivolge ai semiconduttori discreti, il Q200 ai componenti passivi e il Q003 ai circuiti integrati.
All'inizio di questo millennio l'ISO di Ginevra ha promulgato le normative ISO 9000, che affrontano tutti gli aspetti della qualità dei prodotti e della gestione della qualità del lavoro a cui le industrie devono assoggettarsi. Oggi queste norme sono recepite nella più recente versione ISO 9001:2008, che introduce una serie di direttive aggiuntive sulla qualità delle aziende che, oltre agli aspetti tecnici, comprendono anche l'attenzione verso i lavoratori e nei riguardi della sostenibilità ecologica dei processi di fabbricazione e dei prodotti commercializzati. Certamente si tratta di una normativa che qualifica il costruttore come garante della fiducia dei suoi clienti perché capace di operare con le migliori tecnologie disponibili e con i criteri di

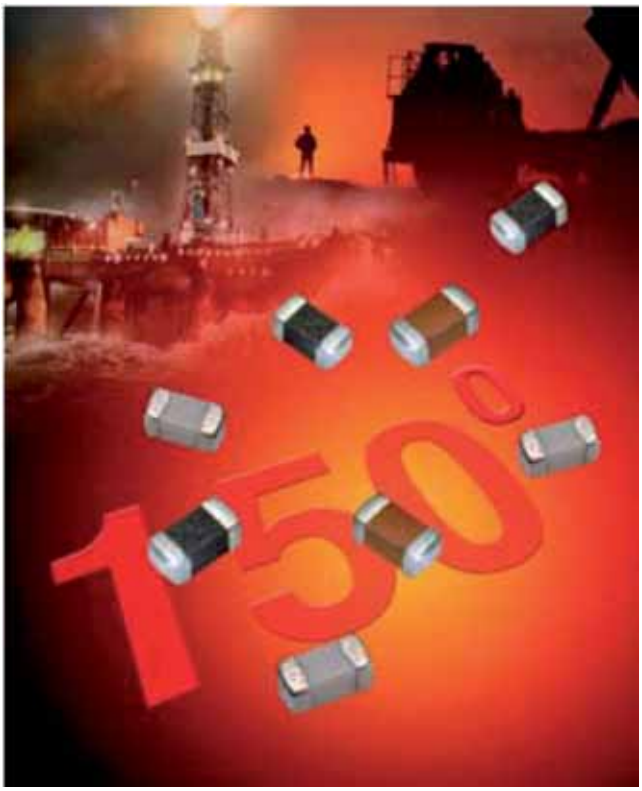


Fig. 2 – I condensatori ceramici multilivello COTS AVX MLCC con dielettrico X8R/X8L e tensione di lavoro fino a 500 V hanno robustezza ben oltre la norma MIL-PRF-55681

Fig. 3 – La soluzione COTS+ per Small Cell Networks PTP 650S di Cambium Networks consente collegamenti point-to-point con velocità dati di 450 Mbps

commercializzazione più attendibili. Dal punto di vista industriale, tuttavia, non obbliga il costruttore a certificare i suoi prodotti in ossequio alle normative militari USA e perciò sono i costruttori stessi che garantiscono le prestazioni dei propri prodotti in termini di robustezza nelle condizioni ambientali più gravose, conformandoli alle usuali norme EN e IEC. Certamente la certificazione militare rimane un obbligo per coloro che hanno trattative commerciali che devono soggiacere al DoD, ma ciò non significa che i loro prodotti siano solo per questo motivo più robusti di quelli degli altri.

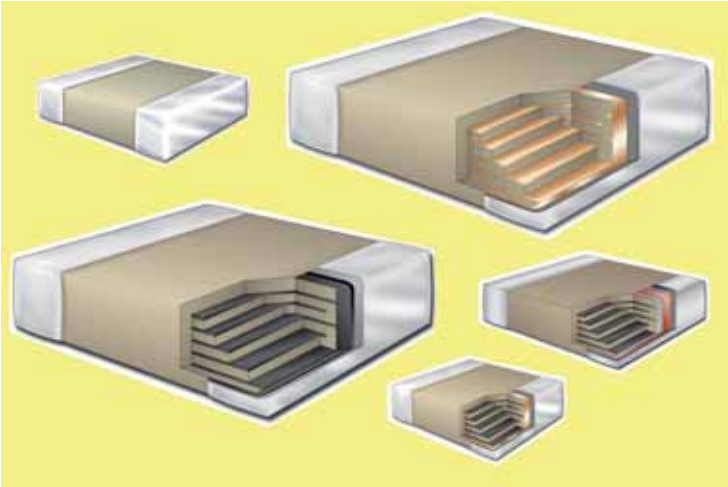


Fig. 4 – Soddisfano le norme AEC-Q200 i condensatori COTS Kemet COG FT-CAP e HV-HT e offrono tensione di lavoro fino a 3 kV e tolleranza termica da -55 a +200 °C

Connettori

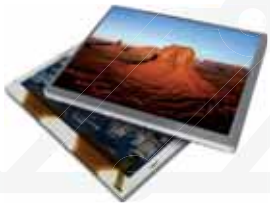
Amphenol produce un'ampia famiglia di connettori COTS con specifiche più severe rispetto alle normative MIL-DTL-38999 e le offre in svariati modelli a contatti singoli, doppi, quadrupli, coassiali e in fibra ottica e con differenti opzioni di package con chiusure a vite, a baionetta, push-pull, a crimp ed ermetiche. Nel ciclo di fabbricazione impiega coperture di fogli di alluminio, di acciaio o di titanio dentro alle quali utilizza inserti di neoprene e per i contatti c'è persino il rame placcato oro avvolto con guaine di silicone, per una tenuta termica di 175 °C che in alcuni modelli arriva a +200 °C. Fra questi connettori COTS si trovano i TV e CTV 38999 serie III per temperature estreme con elevata immunità alle interferenze EMI/RFI, gli SJT 38999 serie I.5 molto leggeri e ad alta densità di contatti, gli LJT 38999 serie I a baionetta molto versatili e a elevata affidabilità nonché i JT 38999 serie II sigillati con prestazioni elevate e un'ampia tolleranza termica. Nel listino ci sono alcuni modelli che ospitano persino 128 contatti.

Condensatori

AVX e **Kemet** fabbricano condensatori COTS+ seguendo procedure interne capaci di andare ben oltre alle normative militari PRF-55365 e 55681. Entrambe producono condensatori al tantalio e condensatori ceramici certificati come adatti tanto alle applicazioni militari quanto a quelle spaziali. AVX ha recentemente introdotto nei suoi condensatori ceramici multilivello MLCC i due nuovi dielettrici X8R e X8L, che soddisfano pienamente la norma 55681 pur rimanendo di tipo COTS. Per questi nuovi componenti i voltaggi vanno da 16 a 500V mentre le capacità va da 10 pF a 22 µF con tolleranza termica estesa da -55 a +150 °C. La società, che fa del gruppo Kyocera, ha recentemente introdotto anche i robustissimi condensatori COTS a banda ultra larga della serie GX0S, capaci di bloccare le componenti continue dei segnali da 16 kHz fino a ben 40 GHz. Kemet ha recentemente introdotto le due serie di condensatori FT-CAP e HV-HT, entrambe per alti voltaggi ed elevate temperature di esercizio. Entrambi a montaggio superficiale e classificati C0G, ossia con variazione di capacità entro ±0,54% fra -55 e +125 °C, questi condensatori sono di tipo ceramico multilivello MLCC e si differenziano perché i primi sono flessibili (FT, Flexible Termination), hanno dielettrico X7R e sono proposti con tensione di lavoro da 500 fino a 3000V e con capacità da 130 pF a 0,33 µF, mentre i secondi (High Voltage-High Temperature) offrono una tolleranza termica estesa da -55 fino a +200 °C con deriva di capacità di ±30ppm/°C e sono proposti per tensioni da 500 a 2000V e capacità da 1 pF a 0,039 µF. Entrambi soddisfano le norme AEC-Q200 pur essendo COTS a tutti gli effetti.

Ponti radio

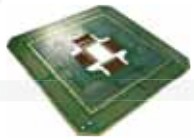
Cambium Networks si è specializzata nello sviluppo e nella fabbricazione di soluzioni "COTS+ Microwave", utilizzabili tanto in ambito militare quanto nell'avionica e oggi anche nelle comunicazioni wireless di ultima generazione. I suoi principali prodotti sono i collegamenti point-to-point (PTP) alla frequenza delle microonde sugli 8 GHz approvati dal DoD oppure alla radiofrequenza sotto i 6 GHz per uso "non DoD". La "backhaul solution" per le Small Cell Networks PTP 650S è capace di garantire una velocità dati di 450 Mbps a una frequenza portante da selezionare fra gli intervalli da 2,5 a 2,6 GHz, da 3,3 a 3,6 GHz, da 4,94 a 4,99 GHz, da 5,15 a 5,25 GHz, da 5,25 a 5,35 GHz, da 5,470 a 5,725 GHz, da 5,725 a 5,850 GHz e da 5,825 a 6,050 GHz. Questi moduli possono essere installati nelle stazioni wireless "non-line-of-sight" (NLOS) con multiplessaggio 2x2 "multiple-input multiple-output" (MIMO) in "orthogonal frequency division multiplexing" (OFDM) e gestire i protocolli 3G e 4G/LTE in un raggio pienamente operativo di circa 2 km. Fra le funzioni di elaborazione includono inoltre la Fast Adaptive Modulation (AMOD) e la Dynamic Spectrum Optimization (DSO).



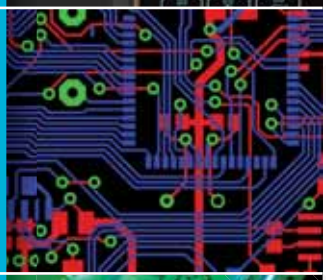
DISPLAY

EMBEDDED
&IPC

OPTOELETTRONICA



PRINTED
CIRCUIT BOARD



DISPLAY
CUSTOM

Mc'TRONIC

Display & Embedded Computing Solutions

Operativa nel settore industriale della visualizzazione (**Display LCD**),
dei **Sistemi Embedded** e **SBC**.
Il **know how**, fondamentale in un ambiente altamente tecnologico
ed in **costante evoluzione**,
è stato assiduamente coltivato per **oltre 25 anni**,
investendo nelle **persone** e nella **ricerca**.

Il riferimento sicuro
per l'innovazione tecnologica

Mc'Tronic S.r.l.
Sede amministrativa - Corso Milano, 180 - 28883 - GRAVELLONA TOCE (VB)
T. +39 0323 86931 r.a. - F. +39 0323 869322
Sede legale - Via Novara, 35 28010 VAPRIO D'AGOGNA (NO)
www.mctronic.it - info@ mctronic.it

Internet of Things: sfide e opportunità

IoT è un'opportunità che permette di creare nuovi modelli di business in maniera "intelligente"

Alexander Damisch
Wind River

Internet of Things (IoT) non è solo una tecnologia, un sistema o un'architettura, è soprattutto un "business case" che richiede una combinazione di tutti questi tre elementi per poter realizzare la sua promessa, ovvero creare nuove opportunità di business in modo più "intelligente". Uno dei principali casi d'uso dell'IoT riguarda la manutenzione preventiva e predittiva. La capacità di diagnosticare accuratamente e prevenire guasti in tempo reale rappresenta un notevole vantaggio competitivo per le aziende ed è essenziale per il funzionamento di infrastrutture critiche. Un guasto di dispositivi e apparati high-tech può rivelarsi molto costoso in termini di spese di riparazione e di mancata produttività che ne deriva. Storicamente, il metodo è sempre stato quello di inviare tecnici a eseguire ispezioni diagnostiche di routine e manutenzione preventiva secondo un programma prestabilito; oltre a essere un processo costoso, non è in grado di garantire che un malfunzionamento non possa verificarsi tra un controllo e l'altro.

Un caso d'uso nel settore delle energie rinnovabili è quello eolico; in questo contesto il "caso estremo" è rappresentato dagli apparati installati in mare aperto. Le turbine eoliche contengono moltissima tecnologia: un generatore, un moltiplicatore di giri e moli circuiti elettronici, inclusi i sistemi di controllo per la regolazione del passo delle pale e molti altri parametri. Se uno qualsiasi di questi elementi si guasta, per esempio per un accumulo di polvere o per l'effetto delle continue vibrazioni, i costi di riparazione saranno molto elevati a causa della dislocazione remota della turbina. Inoltre, siccome le condizioni climatiche saranno sempre un fattore significativo, una turbina potrebbe restare ferma a lungo senza produrre energia.

Per venire incontro a queste esigenze, sistemi on-site equipaggiati con sensori possono raccogliere dati da più turbine (non solamente da una) permettendo di eseguire un'analisi che permetta di prevedere il momento in cui un sistema o un componente potrà guastarsi a causa di stress o surriscaldamento, così da migliorare le attività di manutenzione. Per esempio, se esiste un'elevata probabilità di guasto del moltiplicatore di giri di una turbina, il passaggio a una modalità operativa con prestazioni inferiori ma con carico meccanico ridotto può garantire la continu-

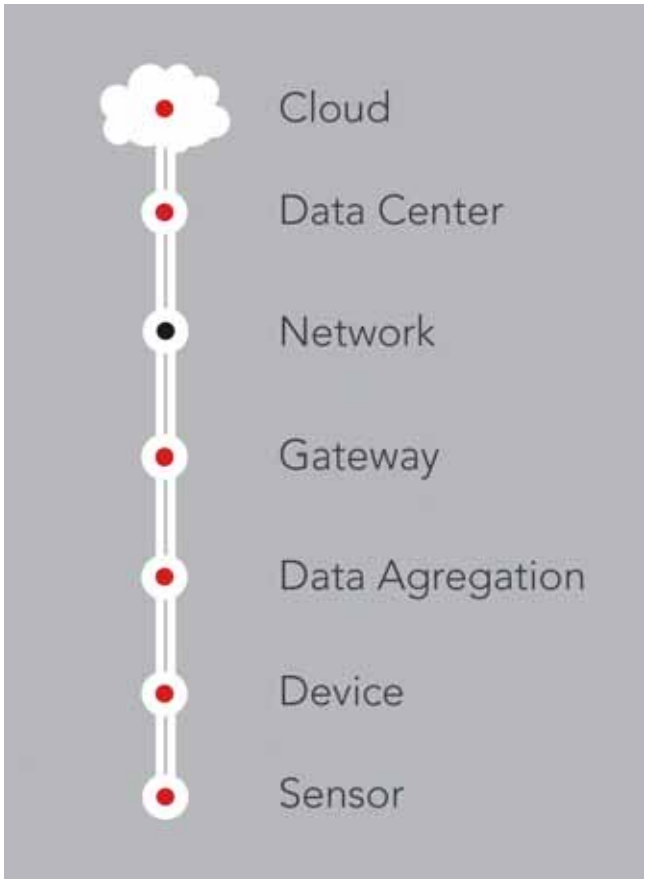


Fig. 1 – Schema di un'architettura IoT end-to-end semplificata

ità di funzionamento – anche se all'80% della capacità – e un'ulteriore generazione di energia per intere settimane. Questo permetterebbe di eseguire una manutenzione programmata che combini la riparazione e il controllo di più di una turbina. Un chiaro esempio dell'importanza del concetto di controllo e di analisi adattativi per raggiungere le migliori prestazioni possibili.

Analisi adattativa

Un altro importante caso d'uso riguarda l'analisi adattativa, quella che comporta il controllo di un sistema nel suo complesso o di un sistema di sistemi. Basata in larga misura sugli stessi dati già raccolti per la manutenzione predittiva, l'analisi adattativa consente ad apparecchiature e dispositivi di analizzare enormi quantità di dati e prendere decisioni in tempo reale per aiutare a migliorare e perfezionare i processi operativi.

Nuove opportunità di ricavo

Le funzionalità di analisi adattativa e di manutenzione predittiva dell'IoT possono giocare un ruolo significativo anche nel creare opportunità per nuove fonti di ricavo, e non solo per ridurre i costi operativi. Nei mercati industriali, per esempio, i grandi player hanno storicamente adottato due modelli di business: quello tradizionale, ossia di vendere dispositivi come sistemi di controllo, motori o interfacce operatore (HMI) oppure vendere soluzioni hardware e software complete comprensive di SLA (Service Level Agreement) per la manutenzione. Entrambi questi modelli di business sono oggi sotto pressione dal punto di vista dei costi con una concorrenza sempre più elevata e margini notevolmente ridotti, specialmente dopo la recente crisi finanziaria che ha portato a una sovrasaturazione nel mercato della produzione di apparecchiature.

Nel caso dei grandi OEM di apparati industriali e automotive, l'enorme base di dispositivi già installati presso i clienti può rivelarsi un fattore critico per l'innovazione. Tuttavia, al di là di nuovi prodotti o nuovi asset, un altro modo per incrementare il fatturato è ottenere nuove entrate ricorrenti legate ai sistemi già venduti e installati. La capacità di innovare e fornire soluzioni semplici che consentano la connessione degli apparati all'IoT può contribuire a ridurre significativamente i costi operativi e fornire valore aggiunto ai clienti attraverso la manutenzione predittiva e l'analisi adattativa. Una fonte di guadagno per i servizi offerti potrebbe essere basato su volume di produzione, numero di dispositivi installati o quantità di dati prestabilite. Questo può dare impulso a un modello di

Iscrivetevi subito
e assicuratevi
i biglietti d'ingresso!
embedded-world.de

Norimberga, Germania
24 – 26.2.2015

embedded world 2015
Exhibition & Conference
... it´s a smarter world

L'incontro per eccellenza
della community embedded!

La manifestazione più grande al mondo per le tecnologie embedded
fa dialogare tra loro tutti gli attori del settore.

Non mancate a un evento che attribuisce un'importanza primaria alla cura dei contatti
e al networking su scala internazionale e al quale si definiscono i trend del domani!

Partner media
Markt&Technik
Elektronik automotive
DESIGN & ELEKTRONIK KNOW-HOW FÜR ENTWICKLER
ENERGIE & TECHNIK
elektroniknet.de
computer-automation.de
energie-und-technik.de
MEDIZIN-UND-elektronik.DE
Elektronik
AUTOMATION
MEDIZIN elektronik

Ente organizzatore del salone
NürnbergMesse GmbH
Tel +49 (0) 9 11. 86 06-49 12
visitorservice@nuernbergmesse.de

Ente organizzatore dei congressi
WEKA FACHMEDIEN GmbH
Tel +49 (0) 89. 2 55 56-13 49
info@embedded-world.eu

NÜRNBERG MESSE

business basato su abbonamenti che comprenda anche il noleggio degli apparati che restano di proprietà del relativo fabbricante.

Un'industria in transizione

Tuttavia, per quanto questo modello possa funzionare bene e senza particolari problemi in alcuni mercati (per esempio molte piccole aziende che stanno muovendosi dalla tecnologia M2M a quella IoT sono già passate dall'addebito in base ai dispositivi all'addebito in base ai volumi di dati o agli specifici servizi di analisi forniti), molti sistemi industriali sono contraddistinti da un elevato livello di integrazione tecnologica, elemento questo che può portare all'insorgere di parecchi ostacoli. Nei mercati dell'automazione di processo e di produzione la raccolta dati è sempre stata condotta attraverso i sistemi di controllo industriale SCADA (Supervisory Control and Data Acquisition). Ma in un sistema SCADA i dati vengono raccolti in maniera statica senza accesso all'informazione in tempo reale, e i protocolli OPC e OPC/UA non sono sufficienti. La realtà è che nell'ultimo decennio buona parte delle apparecchiature per l'automazione è diventata molto più simile a un ambiente di rete nel quale la maggior parte dei parametri viene scambiata tra i dispositivi, principalmente attraverso protocolli industrial Ethernet basati su IP come PROFINET, Ethernet/IP, EtherCAT, TSN o Ethernet POWERLINK. Se per esempio viene installato un gateway o un dispositivo per l'aggregazione dati, questo può diventare un'interfaccia tra i vari dispositivi, anche di quelli progettati solamente per la comunicazione Operations Technology (OT) locale senza essere predisposti per la connessione ai sistemi IT, che non hanno quindi la possibilità di inviare enormi quantità di dati a una piattaforma IoT basata sul cloud. Il gateway introduce un ulteriore elemento critico rappresentato dal perimetro di sicurezza, che fondamentalmente protegge da hacker e altre minacce. Nel settore della generazione di energia esistono gli standard di sicurezza informatica CIP (Critical Infrastructure Protection) creati e gestiti da North American Electric Reliability Corporation (NERC) per gli Stati Uniti; inoltre esistono diversi standard ISA (International Society of Automation) per i mercati dell'automazione e del controllo industriale.

In un ambiente IoT sono essenziali la sicurezza, la personalizzazione e la gestibilità di un sistema, la connetività

I principali requisiti

La sicurezza è un elemento essenziale nell'ambiente IoT per proteggere risorse e apparecchiature dall'esterno nel corso dell'operazione di boot e dell'esecuzione (runtime), e prevenire possibili interruzioni del sistema o potenziali minacce alla sicurezza operativa, pur consentendone la comunicazione con i dispositivi al fine di ottenere i dati necessari.

Un secondo componente necessario è la personalizzazione e la gestibilità di un sistema: il gateway non avrebbe senso se non si potessero gestire dispositivi e piattaforme a causa di piccole variazioni dei parametri di processo. Nella maggior parte delle applicazioni non occorre ricevere dati su centinaia di parametri ogni millisecondo, il sistema deve essere quindi gestito in una fase post-deployment, per esempio attraverso il collegamento a un dispositivo e un'applicazione software che filtri, ad esempio, il volume di informazioni disponibili.

Un terzo requisito essenziale per l'IoT è ovviamente la connettività. Nell'automazione industriale, in particolare, si assiste a una transizione dal vecchio modo di raccogliere i dati ciclicamente o staticamente a una raccolta basata su Ethernet.

I protocolli che stanno affermandosi come standard nell'IoT sono Extensible Messaging e Presence Protocol (XMPP), un protocollo principalmente monodirezionale e quindi molto sicuro, e MQ Telemetry Transport (MQTT), un protocollo per il trasporto del messaging su base publish/subscribe particolarmente utile per comunicare con siti remoti che richiedono un codice compatto.

Nella figura 1, un'architettura IoT end-to-end semplificata mostra la combinazione dei diversi strati che richiedono competenze provenienti da segmenti di mercato differenti. A un'estremità si trovano dispositivi e sensori. I sensori possono essere sensori di parcheggio, sensori del flusso del traffico in una smart city, o azionamenti come le valvole in un'applicazione industriale. Attraverso un collegamento via cavo o un bus si collegano a un dispositivi che viene comunemente chiamato controller.

È qui che oggi la maggior parte dei dispositivi si connette con un sistema SCADA o un aggregatore di dati.

Attualmente questi sono soprattutto sistemi locali di supervisione collegati a controlli implementati staticamente. Sebbene i sistemi moderni possano essere riconfigurati "on-the-fly" per gestire data tag supplementari, richiedono comunque una procedura di "commissioning" e non offrono aggregazione basata su eventi, supportata da un certo livello di "intelligenza" locale dinamica, come ad esempio un algoritmo che possa essere aggiornato in base alle analisi.

Computer rugged orientati alle applicazioni

Grazie a un'innovativa tecnica di smaltimento del calore i computer Perfectron hanno robustezza di livello militare e sono proposti in più versioni per soddisfare un'ampia varietà di ambienti applicativi

Lucio Pellizzari

Cresce la domanda di computer modulari con caratteristiche rugged anche per le applicazioni critiche non tradizionalmente legate ai pochi tipici settori dove questi moduli sono da anni destinati, come il militare, l'aerospaziale e l'industria. I sistemi rugged popolano oggi una gran varietà di ambienti nel medicale, nei trasporti, nella logistica, nella sicurezza e nell'elettronica consumer e ciò ne ha fatto crescere il valore di mercato, stimolando i costruttori a non fabbricare più solo moduli embedded rugged esclusivamente custom ma anche con caratteristiche di versatilità che li hanno finalmente resi multifunzionali e adattabili alle applicazioni. La prima conseguenza di questa nuova tendenza è la graduale discesa dei prezzi, indispensabile per affrontare la competizione nei settori abituati a volumi di vendite molto grandi. La seconda conseguenza è l'inedita proliferazione dei sistemi ibridi con parti rugged e parti commerciali, nei quali sono necessariamente soddisfatti tutti i requisiti mission-critical ma, nel contempo, si trovano installati dispositivi e componenti più economici in tutti quei sottosistemi che non devono essere per forza rugged, in modo tale da offrire un prezzo di vendita finale competitivo. Infine, ci sono sempre più costruttori che allargano la varietà dei settori di destinazione per i loro prodotti, producendo sistemi rugged con caratteristiche dedicate a diversi ambienti applicativi.

Robustezza certificata

Perfectron progetta e produce sistemi embedded rugged caratterizzati dall'affidabilità di funzionamento e dalla versatilità applicativa. Particolarmente efficace è l'innovativa tecnica impiegata per smaltire il calore generato soprattutto dai processori ma anche dai circuiti integrati a maggior densità di transistor. Dentro al cabinet sono installati alcuni tubicini di rame (Copper Heat-Pipe) che veicolano il calore dai componenti più caldi verso le zone periferiche del chip mentre al di sopra sono applicati dei dissipatori (Heat-Sink) con un particolare disegno geometrico detto "High&Low", che favorisce lo spostamento del calore all'esterno. L'effetto congiunto dei tubetti e del dissipatore consente di far sparire dalle schede l'80% del calore e perciò ne assicura il corretto funzionamento anche nelle condizioni più impegnative.

Fig. 1 – I prodotti rugged Perfectron sono certificati MIL-STD-810G e superano i test Wideband Temperature Operation che ne assicurano la piena operatività nell'intero range termico da -40 fino a +85 °C

Grazie a questa tecnica i computer Perfectron fanless (senza ventilazione forzata) sono garantiti per la piena operatività in tutto l'intervallo di temperatura esteso da -40 a +85 °C. Per verificarne la robustezza termica vengono sottoposti ai test Wideband Temperature Operation, che consistono in 500 accensioni e spegnimenti per oltre venti ore ai due limiti di +85 °C e -40 °C, nonché in 48 ore di burn-in per la ricerca dei guasti infantili agli stessi valori limite di temperatura. Dopodiché seguono 1000 on&off a 25 °C e poi 51 ore di burn-in durante le quali la temperatura prima scende da 25 °C a -40 °C, poi risale fino a +85 °C e infine torna a 25 °C. Tutti i dispositivi montati sulle schede Perfectron sono W.T.G.C. (Wide Temperature Grade Component)

e soddisfano la normativa IEC 60068 sull'Environmental Testing. Inoltre, sono di tipo a montaggio superficiale e saldati sulle schede con processi che abbattono gli effetti parassiti e garantiscono la massima protezione meccanica rispetto a urti e vibrazioni. I computer Perfectron sono tutti garantiti contro gli urti fino a 30g o a 50g e contro le vibrazioni di 5 grms e soddisfano le certificazioni tipiche come EN50155 per l'uso nelle ferrovie oppure MIL-STD-810G per l'impiego militare. Per verificarne la robustezza meccanica sono sottoposti a urti di 20g con durata di 11 millisecondi ciascuno ripetuti più volte su tutte le tre direzioni spaziali. Infine, le schede Perfectron sono modulari e dotate del connettore multifunzione StackPC, che consente di impilarle una sull'altra scegliendo di volta in volta lo StackPC-FPE oppure lo StackPC-PC104 per poter aggiungere le interfacce che occorrono alle applicazioni, senza bisogno di riempire di cablaggi l'interno dei cabinet. Oltre ai computer rugged, la società progetta e fabbrica anche schede di espansione, computer a pannello, display a cristalli liquidi, schede grafiche industriali, convertitori di potenza e schede custom PCIe.

Fig. 2 – Innovativa è la tecnica di raffreddamento basata su alcuni tubicini di rame che spostano il calore dai chip più caldi alla periferia del cabinet dove uno speciale dissipatore riesce a far uscire l'80% di tutto il calore interno

Un'unica anima per tre orientamenti applicativi

Fra i computer rugged più recentemente introdotti dalla società si trova SR100 fanless con scheda madre in formato EBX basata sul chipset Intel Haswell QM87 e sul processore di quarta generazione Intel Core i7/i5/i3 Quad-Core con clock di 2,4/1,7 GHz. La scheda viene proposta in due versioni con tolleranza termica da -20 a +60 °C oppure da -40 a +70 °C, proprio per non soddisfare solo le applicazioni militari ma anche l'automazione industriale, il medicale e l'automotive. Nella dotazione di bordo ci sono un disco solido SSD Nano Sata-III con capienza fino a 64 GByte, una memoria Swissbit XR-DIMM espandibile fino a 8 GByte, due DisplayPort, una DVI-I, due Gigabit Ethernet, due USB 3.0, due USB 2.0 e una seriale. Inoltre, nel cabinet da 19" ossia da 250x149x76 mm ci sono due slot di espansione mPCIe e i connettori per aggiungere i moduli supplementari PCIe/104 e/o FPE. L'alimentazione va da 9 fino a 36 Vdc, mentre la robustezza è certificata MIL-STD-810G con immunità agli urti fino a 50g e alle vibrazioni fino a 5 grms. Stesso formato EBX e stessa certificazione MIL-STD-810G per il modello SR200 fanless, basato sullo stesso chipset Intel QM87 ma con sopra un processore Quad-Core Intel i7-4700EQ Haswell e un coprocessore grafico Nvidia GT730M, in grado di pilotare fino a quattro display indipendenti attraverso altrettante interfacce DisplayPort. Nella dotazione si trovano 8 GByte di RAM DDR3 Swissbit XR-DIMM, fino a 64 GByte di SSD SATAIII da 2,5", due Gigabit Ethernet, quattro USB 3.0, una seriale RS232/422/485 e due slot di espansione mPCIe. L'alimentazione è la stessa da 9 a 36 Vdc mentre il cabinet è poco più grande e misura 308x149x76 mm con tolleranza termica anche qui in versione base da -20 a +60 °C oppure estesa da -40 a +75 °C.

Un po' più grande è SR700 fanless che misura 350x230x76 mm e oltre alla certificazione MIL-STD-810G è anche classificato IP65 perché è immune alla polvere e all'acqua grazie ai connettori di tipo M12.

Il processore è ancora Intel Haswell Quad-Core i7-4700EQ con clock di 2,4/1,7 GHz e con attorno il chipset QM87, una RAM Swissbit XR-DIMM da 8 GByte di tipo DDR3 e un SSD SATAIII da 2,5" espandibile fino a 64 GByte. Inoltre, ci sono sei porte di interfaccia impermeabilizzate perché dotate dei connettori M12 e precisamente una VGA, due PCIe Gigabit Ethernet, due USB 2.0 e una seriale.

La tolleranza termica viene anche qui proposta nella versione estesa da -40 a +75 °C oppure nella versione base da -20 a +60 °C e in entrambi i casi con resistenza agli urti fino a 50g e alle vibrazioni fino a 5 grms, mentre l'alimentazione rimane ancora ammessa da 9 a 36 Vdc.

Fig. 3 – Il computer rugged Perfectron SR700 è classificato IP65 e sfrutta il chipset Intel QM87 con processore Quad-Core i7-4700EQ accompagnato da 8 GByte di RAM XR-DIMM e 64 GByte di SSD

Le prospettive di PC/104 nell'era di Internet of Things

Lo standard PC/104 ha saputo rinnovarsi continuamente per accogliere le tecnologie più all'avanguardia pur preservando la sua caratteristica natia di saper gestire la migrazione delle applicazioni senza comportare rischi per gli utilizzatori né costi per gli sviluppatori

Lucio Pellizzari

La recente euforia correlata alla comparsa sul proscenio delle tecnologie per Internet of Things non sembra aver turbato gli esperti del PC/104 Consortium che, dopo oltre 22 anni spesi nello sviluppo delle applicazioni embedded per il formato PC/104, considerate strategiche per l'evoluzione dell'industria, continua a pronosticarne un ruolo centrale e assolutamente determinante in moltissimi ambiti applicativi embedded. Alla sua nascita, il formato PC/104 è stato un importante punto di svolta nell'evoluzione dei computer industriali perché ha spostato l'attenzione degli addetti ai lavori dai sistemi basati su PC di comando ai sistemi di controllo installati direttamente a bordo delle applicazioni. Da questo punto di vista le schede PC/104 sono state fondamentali per sviluppare gran parte delle architetture di interfaccia e delle tecnologie I/O oggi disponibili sul mercato per la messa a punto di un'infinita varietà di sistemi industriali ed è proprio grazie al formato PC/104 che sono state sviluppate e introdotte in commercio le schede rugged con i benefici della modularità, dell'espandibilità, dell'aggiornabilità e della manutenibilità.

Fig. 1 – Il PC/104 Consortium ha saputo continuamente aggiornare il modulo base affinché potessero trovarvi posto i processori, le periferiche e le interfacce basati sulle tecnologie più innovative

Nei moduli PC/104 da 90x96 mm si può trovare di tutto, perché la loro nativa versatilità è stata continuamente rinnovata dal consorzio che ha via via aggiunto nel tempo i supporti per le interfacce e per gli I/O che man mano si diffondevano sul mercato fino ai più recenti PCI-Express dei formati PCIe/104 e PCI/104-Express che includono anche le nuove normative ad alta velocità PCI Express Gen 2 e Gen 3. Invero, questa è una delle attività che impegnano maggiormente il consorzio perché i suoi esperti sono ben consapevoli che il saper stare al passo con i tempi è proprio la caratteristica vincente che ha reso celebre il formato PC/104 e perciò continuano a introdurre prontamente tutti i supporti in grado di consolidarne la fama di standard moderno e sempre attuale. Come esempio si pensi ai numerosissimi supporti introdotti per stare al passo con la prolungata e inarrestabile mutazione che ha riguardato e riguarda ancora i processori Intel e i core ARM.

In ogni caso, la flessibilità dell'impostazione dei bus di sistema è stata determinante affinché nei moduli PC/104 impilati uno sopra l'altro si potessero installare tutti i microprocessori e i microcontrollori introdotti sul mercato: da quelli ad alta velocità a quelli per applicazioni specifiche, da quelli a elevate prestazioni a quelli più economici. Di volta in volta è stato sempre

semplice adeguare la dotazione delle interfacce e degli I/O ai mutevoli requisiti delle architetture x86, ARM o PowerPC e, inoltre, pur continuando a preservare la compattezza dimensionale tipica del formato PC/104 il consorzio ha sempre avuto un occhio di riguardo nel garantirvi l'indispensabile robustezza che costituisce il requisito principale per molte applicazioni non solo del settore industriale ma anche nei trasporti, nel medicale, nell'energia e nell'aerospazio.

Applicazioni senza confini

Oltre a essere rugged, modulari e impilabili, le schede PC/104 sono intrinsecamente versatili e hanno consentito per oltre vent'anni agli OEM di realizzare sistemi standard o custom in grado di soddisfare un'ampia varietà di requisiti termici, elettromagnetici, meccanici e fisici. Oggi il panorama dell'industria elettronica sta cambiando, perché i computer assumono sempre più i connotati di terminali intelligenti portatili, mobili o fissi, connessi senza fili e dislocati ovunque, ininterrottamente ed esclusivamente gestiti attraverso la rete delle reti. In questo contesto anche le soluzioni embedded tipicamente industriali e dedicate a svolgere poche mansioni ma con i severi requisiti dell'assoluta affidabilità e della certezza di risposta in tempo reale stanno cambiando per provare ad adeguarsi all'evolvere delle tecnologie Web.
Internet of Things riguarda il collegamento in rete di un'ampia varietà di dispositivi dai più piccoli sensori intelligenti per il monitoraggio dei parametri medicali o ambientali fino alle centraline di comando sulle macchine utensili in fabbrica o sulle turbine che muovono le navi. Per questo nuovo trend applicativo PC/104 può ancora essere fondamentale perché rimane un punto di riferimento nel mare dei formati standard che cercano di imporsi per le applicazioni locali basate sul Web proprio grazie alla sua capacità di impilare facilmente uno sopra l'altro i moduli con diversi fattori di forma. Il PC/104 Consortium continua ad aggiornare la dotazione e le caratteristiche del formato offrendo i supporti per le nuove interfacce e le nuove tecnologie, ma nel contempo cerca di garantire la compatibilità con tutti gli standard presenti e passati, in modo tale da assicurare ai suoi utenti un percorso di migrazione senza rischi nello spirito di longevità e versatilità che ha reso famose le schede PC/104. Un loro importante valore aggiunto è la facilità con cui si possono implementare le funzioni di protezione e sicurezza indispensabili per le applicazioni IoT e ciò rende i moduli PC/104 ottimi per animare le infrastrutture di rete fondamentali come router, switch e firewall.
C'è un'altra ragione per prospettare una lunga vita per PC/104 ed è legata al disimpiego di Windows XP che purtroppo termina il suo innegabile ruolo di sistema operativo preferito per un'infinità di applicazioni embedded appoggiate alle schede di piccolo formato SFF. Molti sviluppatori di sistemi embedded (e soprattutto quelli non militari) hanno infatti colto l'occasione per abbandonare Microsoft a favore dei sistemi operativi

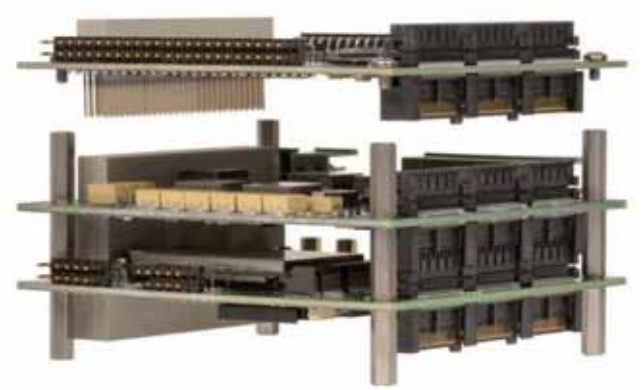


Fig. 2 – L'estrema versatilità delle schede PC/104 e l'impostazione open source dei sistemi operativi Linux ne fanno una coppia ottima per realizzare le infrastrutture di rete fondamentali per Internet-of-Things come router, switch e firewall

Linux considerati più versatili per le applicazioni industriali e scelgono perciò di non passare a Windows Embedded per assegnare un Operating System (OS) o un Real-Time Operating System (RTOS) Linux come Board Support Packages (BPS) nelle proprie schede SFF. La versatilità di Linux permette di gestire facilmente un'ampia scelta di periferiche e agevola la migrazione fra i diversi core ARM e Intel senza bisogno di lunghe fasi di riprogrammazione software o di riconfigurazione hardware sulle schede. Dato che questo vantaggio si sposa con l'intrinseca flessibilità del formato PC/104, ecco che la coppia OS Linux & PC/104 sta diventando la scelta migliore per realizzare SFF adatte a sostituire le numerosissime applicazioni industriali basate su Windows 95 tuttora in attività.
Linux è economico e al pari di PC/104 permette, innanzi tutto, di preservare la compatibilità con le applicazioni già installate e, inoltre, semplifica l'implementazione delle nuove tecnologie man mano che si rendono disponibili sul mercato. Per contro, Windows Embedded offre migliori doti di protezione dati e permette di accorciare il ciclo di sviluppo delle applicazioni grazie a tool di sviluppo più efficaci che aiutano a diminuire il time-to-market. Tuttavia, le prestazioni top non sono sempre l'obiettivo più importante per i sistemi embedded nei quali spesso il requisito primario è quello di offrire una dotazione corretta e adeguata alle esigenze applicative senza inutili e costose ridondanze. Da questo punto di vista la versatilità di Linux è particolarmente adatta per soddisfare l'irrefrenabile evoluzione dei core ARM che da molti anni richiede ai sistemi operativi di essere non solo a passo con i tempi ma anche intercambiabili nelle parti essenziali, senza rischi per le prestazioni. Sia Linux sia PC/104 sono modulari ed espandibili e ciò li rende adatti per tutte le applicazioni da quelle consumer usa e getta fino a quelle più grandi che coinvolgono onerosi investimenti e a maggior ragione anche per le prossime venture applicazioni Internet-of-Things.

IDE, un tool versatile e indispensabile

Francesco Ferrari

Gli ambienti di sviluppo integrati per applicazioni embedded sono decisamente numerosi, molto versatili e sempre più articolati, per raggiungere l'obbiettivo di semplificare il lavoro di sviluppo

Gli sviluppatori sono spesso alla ricerca di ambienti di sviluppo integrati (IDE) in grado di soddisfare le loro esigenze specifiche, e le possibilità di scelta sono diventate ormai davvero numerose. Molti preferiscono usare editor di testo avanzati che rendono la programmazione più semplice oppure dispongono di funzionalità particolari e, di fatto, ci sono IDE per qualsiasi linguaggio di programmazione con cui si desideri lavorare. Ci sono anche molte integrazioni cross-IDE, con diversi tipi di tool, che aumentano notevolmente la flessibilità di questi ambienti. La parte più importante di un IDE è l'integrazione del software, solitamente editor, compilatore e debugger, che permette di preparare e rendersi conto di come funzioni effettivamente il codice che viene eseguito su un hardware embedded (o di un qualsiasi altro tipo di applicazione). Uno dei principali vantaggi di un IDE è la capacità di identificare eventuali problemi che si possono presentare con il codice e evidenziarne le parti critiche. Funzioni avanzate, inoltre, possono accelerare lo sviluppo di segmenti di codice particolarmente critici.

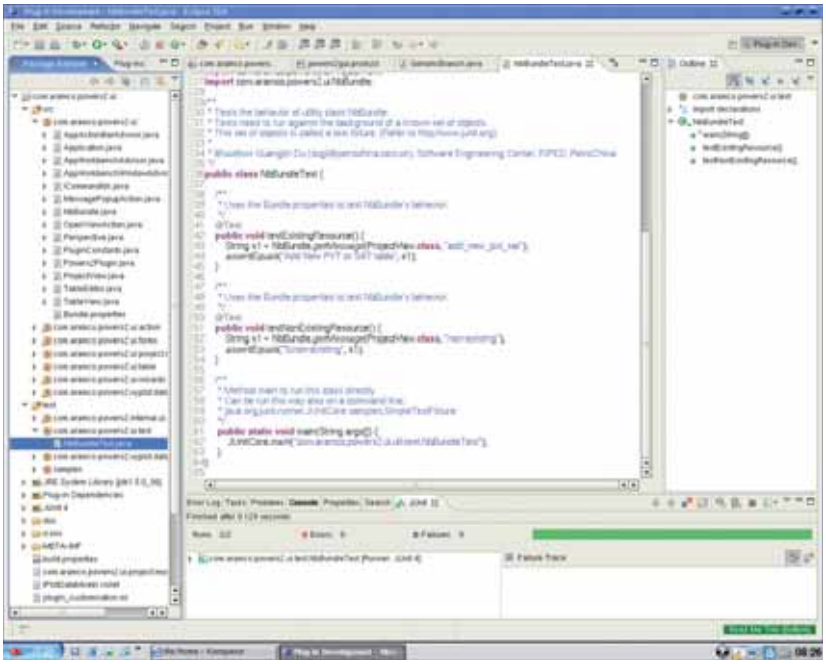


Fig. 1 – Tra i più diffusi IDE per lo sviluppo embedded, specialmente per ARM, c'è la piattaforma Eclipse, usata anche come base per numerosi IDE proposti dagli OEM

Pro e contro

La combinazione di editor, compilatori, debugger e altri tool in un unico IDE permette di aumentare la produttività quando si sviluppano applicazioni embedded, ma ci possono essere anche alcuni inconvenienti. Molti sviluppatori, per esempio, hanno un flusso di lavoro ben definito e sono ormai abituati da tempo a utilizzare una serie di tool che conoscono bene. Non stupisce quindi che cambiare in modo drastico il workflow con uno nuovo IDE è una soluzione che spesso non viene accolta con molto entusiasmo. A

Fig. 2 – La versione più recente di NetBeans è la 8.0.1 che mette a disposizione, fra l'altro, un analizzatore di codice e degli editor per lavorare con la più recente tecnologia Java

questo va aggiunto che occorre investire del tempo per imparare a usare al meglio i nuovi tool (la curva di apprendimento), periodo in cui la produttività inevitabilmente non può essere quella massima.
L'obbiettivo principale di questi tool integrati resta comunque quello di semplificare e rendere più veloce il lavoro di sviluppo e debug, eliminando, per esempio, le attività ridondanti che richiedono molto tempo prezioso.
C'è anche qualcuno che sostiene che questa facilità d'uso indotta dall'impiego degli IDE sia un punto a loro sfavore dal punto di vista dell'opportunità di adozione. Alcuni ritengono, infatti, che un IDE per lo sviluppo di progetti embedded potrebbe non essere la scelta giusta per uno sviluppatore professionista e a supporto di questa tesi viene addotta proprio la notevole facilità che gli IDE offrono per sviluppare un codice, anche senza conoscere fino in fondo tutte le implicazioni di ciò che si sta facendo. Gli IDE infatti permettono di ottenere dei risultati anche senza conoscere tutti i dettagli dei tool come i compilatori e dei processi di generazione del codice. Questo punto potrebbe essere condivisibile nel caso gli IDE siano usati a scopi didattici, dove l'obbiettivo non è tanto generare del codice quanto apprendere il più a fondo possibile le funzionalità dei tool e i processi di generazione del codice.

Scegliere in IDE

La disponibilità di IDE è molto ampia: alcuni sono messi a disposizione gratuitamente dagli OEM per favorire la diffusione dei rispettivi componenti, altri sono disponibili come open source, mentre altri, infine, devono essere pagati. Anche Microsoft propone il suo IDE Visual Studio.
La scelta di un IDE spesso non è affatto semplice visto che occorre prendere in considerazione diversi parametri. Per esempio, occorrerebbe avere le idee chiare su che cosa ci si aspetta realmente da un IDE, anche in prospettiva nel medio termine, e capire vantaggi e svantaggi di ciascun IDE che potenzialmente si intende adottare.
Gli elementi più critici nella scelta di un IDE sono relativi al supporto dell'hardware, visto che spesso si possono utilizzare solo con alcune famiglie di componenti. Questo pone il problema, non irrilevante, che quando si affrontano progetti complessi, con più componenti diversi, occorre spesso utilizzare più IDE, con i relativi problemi legati alle curve di apprendimento per i singoli IDE e al passaggio da uno all'altro. Esistono comunque IDE multipiattaforma in grado di supportare un numero decisamente elevato di componenti e quindi non è raro il caso in cui diventa possibile usare un unico IDE per tutto il progetto, raggiungendo quindi l'obbiettivo di migliorare la produttività.
In generale, occorrerebbe comunque verificare quali librerie e periferiche che possano accelerare il progetto siano in grado di supportare l'IDE che si intende utilizzare. Questo significa ovviamente anche verificare che l'IDE prescelto supporti tutti i componenti scelti per il progetto, come microcontroller, processori, FPGA eccetera. Occorre anche chiedersi quanto gli sviluppatori dedicati al progetto abbiamo familiarità con l'IDE che si sta valutando e quale tipo di supporto viene fornito da produttore e community, un aspetto che diventa molto importate per non vanificare i benefici dell'uso degli IDE sul versante dei tempi di sviluppo dei progetti.
Per quanto riguarda gli elementi che compongono l'IDE, andrebbe verificata, per esempio, anche la disponibilità e la qualità dei tool per valutare le prestazioni del codice generato, in modo da poter realizzare velocemente applicazioni performanti.
Gli IDE citati nelle prossime pagine non sono classificati in un ordine particolare di qualità o importanza, ma sono semplicemente alcuni esempi, assolutamente non esaustivi visto che l'offerta è davvero molto ampia, di questo variegato mondo.

Alcuni esempi

Tra gli IDE multipiattaforma che supportano lo sviluppo di diverse architetture ci sono Eclipse, NetBeans e IAR Embedded Workbench.

Eclipse è sicuramente uno dei più diffusi, anche perché molte delle soluzioni degli OEM si basano su questa piattaforma. Per esempio il progetto CDT fornisce i tool per un IDE per C e C++ basato sulla piattaforma Eclipse. Tra le funzionalità sono comprese quelle per la creazione di progetti e per diverse toolchain, macro definition browser, editor con evidenziatori di sintassi, navigazione con hyperlink, generazione di codice, visual debugging e molte altre. Per quanto riguarda gli sviluppi più recenti, la community IoT (Internet of Things) di Eclipse ha rilasciato un Open Stack IoT per Java in grado di semplificare lo sviluppo di applicazioni IoT anche tramite il riutilizzo di core e set di framework e servizi.

Per quanto riguarda NetBeans, il download più recente disponibile è la versione 8.0.1 che introduce diverse novità rispetto alla precedente versione 8.0. NetBeans IDE 8.0.1 mette a disposizione un analizzatore di codice e degli editor per lavorare con la più recente tecnologia Java (Java SE 8, Java SE Embedded 8 e Java ME Embedded 8). Questa release, inoltre, migliora il supporto per Maven e Java EE con PrimeFaces e aggiunge nuovi tool per l'HTML5, in particolare per AngularJS. Nella release 8.0.1 è stato migliorato anche il supporto per PHP e C/C++.

Un altro ambiente diffuso per lo sviluppo di progetti embedded è IAR Embedded Workbench, anche perché supporta diverse famiglie di componenti di produttori come ARM, Atmel, Freescale, Maxim, National, Renesas, Samsung, STMicroelectronics e Texas Instruments. In realtà IAR Embedded Workbench è una articolata toolchain che comprende numerosi strumenti.

Gli annunci più recenti per questo prodotto sono relativi all'introduzione della versione 7.30 dell'IAR Embedded Workbench per ARM in grado di supportare i nuovi core Cortex-M7.

Per gli IDE degli OEM ci sono diversi esempi, come l'High Performance Embedded Workshop di Renesas che offre un IDE GUI-based per lo sviluppo e il debugging di applicazioni embedded basate sui microcontroller Renesas (SuperH, M32R, M16C, R8C, H8SX, H8S, e H8). Questa suite di tool integra una interfaccia utente standard, compilatori C/C++ e debugger per diverse piattaforme, oltre agli emulatori e altri strumenti.

Per il segmento embedded è disponibile inoltre Renesas Eclipse embedded studio, noto anche come e² studio, un completo ambiente di sviluppo e di debug basato sul progetto CDT Eclipse. Questo ambiente permette di integrare numerosi compilatori per consentire agli sviluppatori di scegliere i tool più idonei. Code Composer Studio è invece l'IDE che supporta i microcontroller e i processori embedded di TI. Questo IDE comprende una suite di tool per lo sviluppo e il debug di applicazioni embedded che comprende compilatore C/C++, un editor per il codice sorgente, debugger, profiler e diverse altre funzionalità. In pratica Code Composer Studio riesce a combinare i vantaggi di un framework Eclipse con le capacità di debug dei tool TI. La versione più recente è la v6 di fine aprile 2014. Un altro esempio di IDE dedicato al segmento embedded è emIDE. Questo sistema gratuito offre le funzionalità necessarie per sviluppare e testare applicazioni professionali embedded.

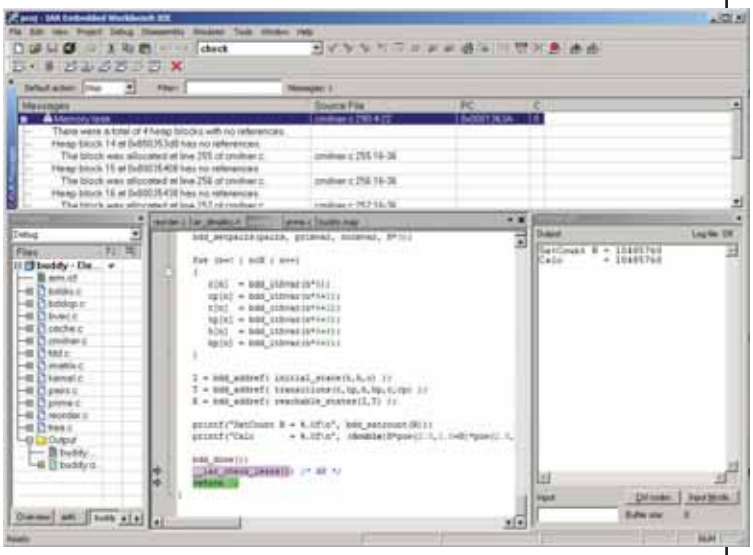


Fig. 3 – IAR Embedded Workbench è una articolata toolchain che comprende numerosi strumenti

Per quanto riguarda le piattaforme, la compatibilità è verso ARM/Cortex, PIC32 (MIPS) e i Renesas RX. Questo IDE integra il supporto per il debug con J-Link/J-Trace che consente il download e diretto e il debug delle applicazioni in RAM o nella memoria Flash (fra l'altro, è possibile inserire un numero illimitato di breakpoint anche quando si effettua il debug in Flash).

CrossCore Embedded Studio è un altro IDE per le famiglie di processori Blackfin e SHARC di Analog Devices. Questo IDE basato su Eclipse utilizza i tool più recenti per generazione del codice.

uomini & imprese

Gli uomini che fanno le imprese

STRATEGIE • MACROECONOMIA • NUOVI MERCATI • INTERNAZIONALIZZAZIONE • FINANZA • FORMAZIONE • INNOVAZIONE

La rivista per il management

Sensori industriali ottici

Lucio Pellizzari

Fra i sensori più diffusi nell'automazione industriale i dispositivi ottici consentono le ispezioni a distanza anche negli ambienti inquinati e poiché sono semplici da installare e configurare, sono perciò preferiti a molti altri tipi di sensori

Malgrado l'impressionante perfezionarsi delle tecnologie di fabbricazione industriale, ancora oggi nessun ciclo produttivo può dirsi esente da imperfezioni ma, fortunatamente, al pari delle tecniche di lavorazione e assemblaggio si sono evolute anche le metodologie per l'individuazione rapida dei difetti, accompagnate dall'indispensabile immediata correzione che consente poi di garantire la massima qualità dei prodotti pretesa nei requisiti. In pratica, sono i sensori industriali che rilevano i difetti di lavorazione nei prodotti mentre il sistema di controllo automatico provvede a classificarli e a indirizzarli verso il loro adeguato percorso di recupero.

Molti di questi sensori sono ottici, perché consentono le ispezioni a distanza e sono oggi disponibili in un'ampia varietà di modelli e configurazioni, in grado di utilizzare tecniche di riconoscimento adattative che migliorano continuamente la loro qualità operativa, aggiornando automaticamente la base di conoscenze man mano che vengono rilevati i difetti nei prodotti. In pratica, i sensori ottici acquisiscono le immagini che un software di elaborazione grafica visualizza su display e processa numericamente effettuando il confronto con immagini note per stabilire la presenza dei difetti visibili, ma quest'impostazione generica assume ovviamente una varietà di configurazioni pratiche che si adattano alle applicazioni e assecondano le tecnologie sviluppate dai costruttori. L'affidabilità e la precisione dei sensori ottici sono fattori decisivi sulla qualità e sui costi dell'intero moderno sistema produttivo e perciò devono soddisfare requisiti di robustezza severi a sufficienza per poter operare negli ambienti industriali, piuttosto che a bordo dei treni o negli impianti delle centrali elettriche.

Il loro vantaggio è la rilevazione degli oggetti senza contatto in qualsiasi condizione di inquinamento ambientale e oggi se ne possono trovare nella forma di sensori fotoelettrici meglio noti come fotocellule a sbarramento, a riflessione, a tasteggio, a forcella o a telaio oppure come fotosensori in fibra ottica per il rilevamento degli oggetti molto piccoli in spazi ridotti oppure ancora come sensori di contrasto e lettori di colore ottimi per le catene automatizzate d'imballaggio e stampa, ma ce ne sono anche configurati come misuratori di distanze che effettuano calcolando il tempo di volo (TOF, Time-Of-Flight) di opportuni impulsi ottici dalla sorgente agli oggetti e ritorno.

Più sofisticati sono i sensori di immagine che consentono di rilevare i dettagli più piccoli delle superfici, identificare codici e caratteri nonché riconoscere la composizione chimica dei materiali.

Microscan sviluppa e produce da oltre 30 anni soluzioni per l'acquisizione e il controllo dati delle quali detiene numerosi brevetti. La nuova Vision MINI Xi è una smart camera per l'elaborazione elettronica delle immagini che misura 25,4x45,7x53,3 mm, pesa 91 grammi e integra una porta Ethernet, una seriale RS-232, un I/O optoisolato e un adattatore per l'alimentazione da 10 a 30 Vdc. La velocità è di 60 fps in formato WVGA da 752x480 pixel, 15 fps in SXGA

Fig. 1 – La piccola smart camera Microscan Vision MINI Xi per la scansione e l'elaborazione delle immagini industriali con riconoscimento dei simboli 1D/2D e dei caratteri OCR

da 1280x1024 pixel e 5 fps in QXGA da 2048x1536 pixel. Il software di visione artificiale AutoVision nella sua recente release 3.0 consente di configurare svariate funzioni come la scansione a breve distanza, l'identificazione automatica dei simboli 1D/2D e il riconoscimento ottico dei caratteri (OCR). È ideale per l'ispezione industriale in spazi angusti con la contemporanea lettura dei codici a barre.

Omron ha da poco compiuto 80 anni e festeggia introducendo una nuova serie di sensori per l'automazione industriale. I sensori fotoelettrici M18 E3FC garantiscono un'elevata protezione rispetto ai detergenti (standard Ecolab e Diversey) durante i

Fig. 2 – Grazie all'elevato grado di protezione termica e resistenza ai detergenti i sensori fotoelettrici Omron M18 E3FC sono ideali per le industrie di Food & Beverage

lavaggi ad alta pressione e sono perciò ideali per le industrie di lavorazione di alimenti e bevande (Food & Beverage). Sono certificati IP68/IP69K e garantiti nelle temperature da -25 a +55 °C anche a contatto con detergenti aggressivi oppure sottoposti a shock termici grazie alla custodia in acciaio AISI316L e alla resina epossidica all'interfaccia fra connettore e cavo che impedisce l'ingresso dei contaminanti. Hanno un potente LED rosso che ne semplifica l'allineamento e sono disponibili in svariati modelli a sbarramento, a soppressione dello sfondo, a riflessione e reflex da 300 mm e da 1 mt.

On Semiconductor ha presentato un nuovo sensore d'immagine CCD a elevate prestazioni specificatamente progettato per le applicazioni di imaging industriali. KAI-08670 incorpora 8,6 Mpixel con formato ottico APS-H che consente di acquisire immagini di qualità per i sistemi di visione industriali e medicali, la videosorveglianza, il controllo del traffico e la logistica. Il sensore amplia la famiglia dei sensori Interline Transfer CCD TrueSense con pixel da 7,4x7,4 micron che offre nella misura di 3600 in orizzontale e 2400 in verticale per un'immagine attiva di 26,64x17,76 mm con diagonale di 32 mm. La gamma dinamica viene aumentata da 70 dB fino a ben 82 dB su tutte e quattro le uscite da 12 frame al secondo con sensibilità da 9,7 a 33 µV e, inoltre, viene fornito insieme alla tecnologia TrueSense Sparse Color Filter Pattern che permette di massimizzare la percettibilità

Fig. 3 – Il sensore d'immagine CCD KAI-08670 è proposto da On Semiconductor per i sistemi di visione industriali e medicali con formato ottico APS-H

luminosa in tutta la gamma cromatica. Il package è CPGA71 da 72 pin e misura 47,24x45,34 mm.

Pepperl+Fuchs sviluppa e produce tecnologie per l'automazione e svariati tipi di sensori ottici industriali. Nuove sono le tre fotocellule a tasteggio miniaturizzate della serie ML100 ideali per l'uso in spazi ristretti con un elevato livello di affidabilità. ML100-8-W ha un ampio spot luminoso che evita gli errori sulle superfici estremamente ruvide ed è molto resistente alle vibrazioni e indipendente rispetto all'inclinazione degli oggetti. La versione ML100-8-HW con valutazione dello sfondo sfrutta il principio della triangolazione per distinguere fra un oggetto vicino e uno lontano, mentre la ML100-8-H è a soppressione dello sfondo e può rilevare le proprietà di un oggetto ignorando le interferenze attorno come la polvere. Lo scanner a LED multiplo E2100 sfrutta la Pulse Ranging Technology per effettuare misurazioni bidimensionali su aree con qualsiasi dimensione e anche sulle superfici irregolari.

Specim nasce dopo una decina d'anni di collaborazione fra la NASA e il locale VTT Technical Research Centre spesi per sviluppare e realizzare all'inizio degli anni '90 il primo spettrografo iperspettrale. Questa tecnologia consente di rilevare le informazioni spaziali e spettrali degli oggetti acquisendo simultaneamente più immagini in bande spettrali contigue per sovrapporle in cubi iperspettrali che

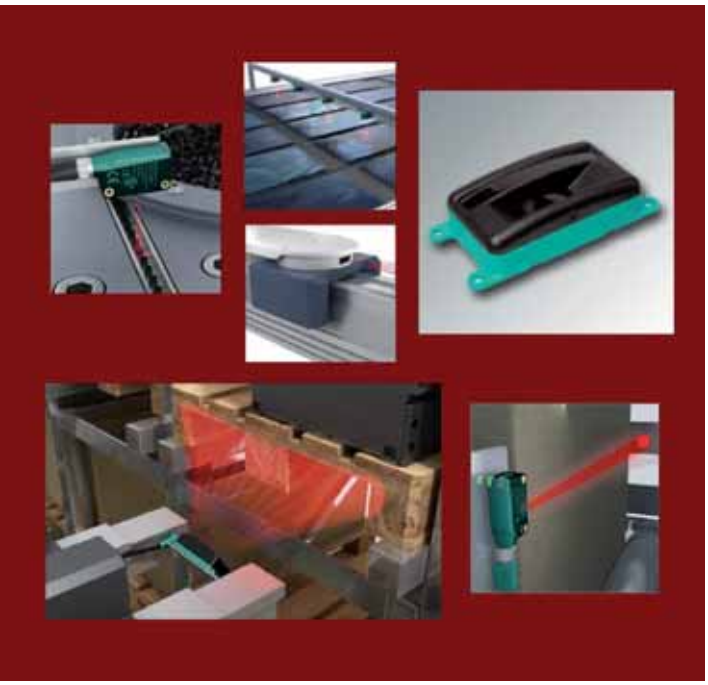


Fig. 4 – Le fotocellule a tasteggio ML100 e lo scanner a LED multiplo E2100 che Pepperl+Fuchs propone per le misure ottiche industriali indipendenti dalle condizioni ambientali

Fig. 5 – La telecamera per imaging iperspettrale Specim ImSpector V10M consente di acquisire simultaneamente le informazioni spaziali e spettrali individuando la composizione chimica dei materiali

consentono di individuare, per esempio, il vapore acqueo, l'inquinamento, la composizione minerale e la temperatura negli strati volumetrici dei materiali. Oggi Specim offre un'ampia gamma di spettrografi sia per le ispezioni atmosferiche da satellite sia per l'imaging spettrale nelle applicazioni industriali dove consentono di distinguere fra la plastica, il vetro, i metalli, gli alimenti, i medicinali e persino i rifiuti. Per le prestazioni più sofisticate ImSpector V10M offre una gamma spettrale sui pixel che va da 350 fino a 1000 nm con una risoluzione di 1,5 nm e dimensioni "cubiche" delle immagini di 7,0 mm per le informazioni spettrali e 24,0 mm per quelle spaziali.

Tattile sviluppa e produce da oltre 20 anni sistemi di visione artificiale e telecamere intelligenti nelle tre categorie di prodotto Industrial, Traffic e Railway. Recentemente ha introdotto la telecamera lineare CameraLink Serie TAG-7 dedicata alla visione artificiale nelle applicazioni in cui è richiesta un'elevata qualità dell'immagine. Il sensore ottico CCD ha 2 Mpixel da 14x14 µm con clock di 22 MHz, risposta spettrale che va da 200 fino a 1000 nm e profondità di 8 bit per pixel. Compatibile con gli standard CameraLink e GenIcam la camera può integrarsi facilmente con i software di visione più diffusi e grazie all'Fpga Altera 40 KLe può eseguire molteplici algoritmi di pre-elaborazione in tempo reale. Può essere sincronizzata con un trigger esterno mentre le dimensioni sono di 62x62x36 mm con l'alimentazione ammessa a 12 oppure a 24 Vdc.

Fig. 6 – Hanno risposta spettrale da 200 a 1000 nm i pixel da 14x14 µm della telecamera lineare Tattile CameraLink Serie TAG-7 per le applicazioni di visione artificiale

Fig. 7 – Può rilevare gli oggetti fino a 5 metri di distanza la fotocellula laser a tempo di volo SensoPart FT 55-RLAP consigliata da Tritecnica in diverse opzioni orientate alle applicazioni

Tritecnica offre sul mercato italiano da oltre mezzo secolo prodotti per l'automazione industriale, la sicurezza e la logistica tecnologicamente innovativi.
Nell'ampia gamma dei sensori d'immagine e di visione ha aggiunto una nuova camera fotoelettrica interamente progettata e fabbricata a Wieden, nella teutonica foresta nera, da SensoPart che festeggia quest'anno 20 anni di specializzazione nella sensoristica per l'automazione industriale. La fotocellula FT 55-RLAP è pensata per le misure a distanza di oggetti difficili come pezzi scuri, irregolari o molto curvi che effettua calcolando il tempo di volo degli impulsi emessi dal laser rosso fino a 5 metri oppure da un LED rosso in diverse opzioni da 1,2 fino a 25 metri.
A bordo ci sono anche due uscite digitali con soppressione dello sfondo a 500 Hz, ma una può essere riconvertita come uscita analogica.
Le dimensioni sono di 50x50,08x23 mm con 125 grammi di peso e l'alimentazione va da 12 a 30 Vdc.

sps ipc drives
ITALIA

Tecnologie per l'Automazione Elettrica
Sistemi e Componenti
Fiera e Congresso
Parma, 12-14 maggio 2015

Efficienza e produttività

L'automazione per l'industria ti aspetta in fiera

Prodotti e Soluzioni

Sistemi e componenti di azionamento
Infrastrutture meccaniche
Sensori
Tecnologia di controllo
IPC
Software industriale
Tecnologia di interfacciamento
Dispositivi di commutazione in bassa tensione
Dispositivi di interfaccia uomo-macchina (HMI)
Comunicazione industriale
Formazione e consulenza
System Integrator

Per info:
Tel +39 02 880 778.1
espositori@spsitalia.it
www.spsitalia.it

messe frankfurt

Tecnologie basate su Internet per le smart grid

Come implementare i protocolli di ridondanza HSR e IEEE 1588 PTP con i SoC FPGA di Altera su cui gira il sistema operativo Linux

Jouni Kujala
Flexibilis Oy
Tampere, Finland

Fig. 1 – Scheda di sviluppo SoC e scheda SFP di Terasic

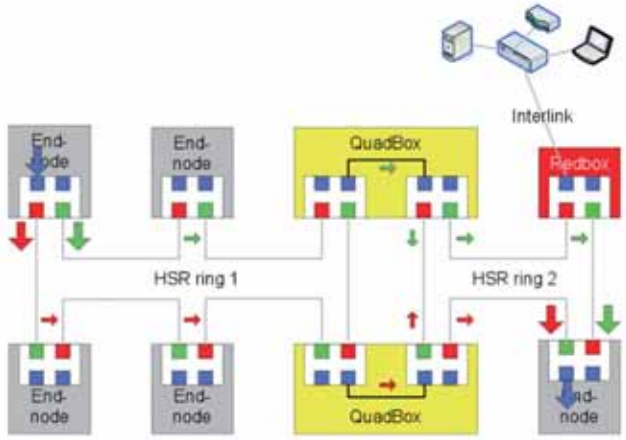
Il termine "smart grid" identifica una moderna rete elettrica che sfrutta un certo numero di nuove tecnologie per la raccolta di informazioni, la comunicazione e il controllo della rete stessa.
Oltre a garantire una migliore efficienza e una maggiore affidabilità, una smart grid consente una generazione distribuita dell'energia, semplificando il collegamento di sorgenti di energia rinnovabili diversificate, come ad esempio l'energia fotovoltaica o quella eolica, alle rete. Tra le nuove tecnologie impiegate nelle smart grid di possono segnalare i protocolli HSR (High -Availability Seamless Redundancy) e IEEE 1588 PTP (Precision Time Protocol) utilizzati nelle sottostazioni per la comunicazione interna e la sincronizzazione temporale delle misure elettriche.
In questo articolo è proposta l'implementazione dei protocolli HSR e IEEE 1588 PTP mediante il SoC Cyclone V di Altera su cui gira il sistema operativo Linux. Il chip integra una struttura FPGA e un processore hard basato su ARM. La soluzione proposta può essere usata sia per lo sviluppo di nuovi progetti sia per l'aggiornamento di dispositivi esistenti.
Nella figura 1 è riportato un esempio di implementazione dei protocolli HSR e IEEE 1588 PTP che sfrutta un SoC della serie Cyclone. Nella figura sono rappresentate due schede PCB, entrambe già disponibili: quella di maggiori dimensioni è la scheda di sviluppo Cyclone V SX di Altera, mentre quella di dimensioni inferiori è la scheda SFP-HSMC di Terasic che si collega al connettore HSMC della scheda SoC e mette a disposizione slot SFP (Small Form-factor Pluggable) per collegamenti Ethernet in fibra o in rame, in funzione del tipo di modulo. Nella figura 2 è riportato lo schema a blocchi delle due schede.
Il nucleo centrale di questa implementazione è rappresentato dallo switch HSR che effettua l'inoltro (forward) dei frame HSR/Ethernet da porta a porta. Nell'implementazione presa in considerazione vi sono quattro porte, una delle quali è collegata al processore ARM di tipo hard, in modo da consentire l'invio e la ricezione di frame Ethernet. Le restanti porte HSR/Ethernet sono connesse, attraverso blocchi di adattamento GMII-1000BASE-X e (G)MII-SGMII, ai moduli SFP e ad altri dispositivi. Un numero di porte esterne pari a tre è sufficiente per l'implementazione di RedBoxes (box di ridondanza) dedicati (maggiori informazioni nel riquadro:

HSR: informazioni di base

HSR è un protocollo di ridondanza per reti Ethernet. In maniera analoga a quanto previsto da RSTP (Rapid Spanning Tree Protocol), la ridondanza è garantita dalla presenza di collegamenti aggiuntivi nella rete. A differenza di RSTP, HSR non disabilità questi link aggiuntivi durante il funzionamento. Al contrario, una rete HSR utilizza tutti i link per tutto il tempo mentre i nodi eseguono copie dei frame per utilizzare contemporaneamente tutti i percorsi di rete. Mentre RSTP disabilita alcuni link selezionati per dar vita a una rete priva di anelli, una rete HSR prevede la presenza di anelli.

Nelle reti HSR, ai frame Ethernet è aggiunta un'intestazione HSR (header). L'intestazione contiene un numero di sequenza che, abbinato a all'indirizzo del MAC sorgente è utilizzato per il riconoscimento delle copie dello stesso frame. I nodi nella rete HSR rilevano e memorizzano i frame che hanno ricevuto e inoltrato in precedenza, in modo da rimuovere le copie aggiuntive dei frame dalla rete. Si tratta di un'operazione necessaria al fine di evitare il verificarsi di un "loop infinito" che consuma tutta la capacità disponibile. Poiché i link della rete non sono disabilitati dal protocollo di ridondanza, quest'ultimo non richiede un tempo di ripristino in caso di guasto. Il protocollo HSR rappresenta dunque la scelta migliore per tutte quelle applicazioni per le quali non è ammessa alcuna interruzione nelle comunicazioni: avionica, distribuzione di energia elettrica, militare sono alcuni esempi tipici.

La topologia tipica di una rete HSR è un anello, o parecchi anelli connessi gli uni altri altri. In ogni caso la tecnologia HSR non è limitata a questo tipo di topologia, bensì supporta qualsiasi topologia. Va comunque evidenziato il fatto che l'implementazione di reti HSR di grandi dimensioni (con centinaia di nodi) non è consigliata, poiché tutto il traffico transita in ogni nodo di una rete HSR, a meno che non sia limitato ad esempio da una LAN virtuale. Esaminando lo schema di una tipica rete HSR, si può osservare la presenza di RedBox (box di ridondanza) che collegano nodi non-HSR e segmenti di rete alla rete HSR. I QuadBox, invece, connettono gli anelli HSR gli uni agli altri. I nodi terminali (noti anche come DANH) sono i nodi di comunicazione per i quali la rete è costruita. Una rete HSR supporta inoltre in modo nativo il collegamento a reti PRP mediante i box di ridondanza HSR-PRP.



Schema di una rete HSR

"HSR: informazioni di base"). In ogni caso è utile avere una porta aggiuntiva nei nodi terminali, da utilizzare ad esempio come porta di manutenzione o per implementare la funzionalità "RedBox-in-EndNode", grazie alla quale è possibile eliminare il ricorso a RedBoxes dedicati.

I blocchi adattatori modificano l'interfaccia nativa MII/GMII dello switch HSR in un'interfaccia 1000BASE-X o SGMII. La prima è utilizzata quando un modulo gigabit in fibra ottica è connesso a uno slot SFP. L'interfaccia 1000BASE-X può essere utilizzata anche con moduli SFP per connessioni con i tradizionali cavi in rame, anche se le velocità di trasmissione più basse (10 e 100 Mbps) sono supportate solo in modalità SGMII. Poiché i moduli SFP per connessioni in rame sono progettati per sostituire direttamente i moduli per le connessioni in fibra ottica, essi devono essere controllati in maniera separata per poter operare in modalità SGMII. Il comando per commutare in modalità SGMII è inviato al chip per il livello fisico (PHY), presente all'interno del modulo mediante un bus I2C controllato attraverso il blocco GPIO (General Purpose Input/Output).

Il blocco RTC (Real-Time Clock) è preposto alla misura del periodo di clock attuale. Il periodo di clock è necessario per implementare la funzionalità IEEE 1588 PTP. Il blocco in real time è separato dallo switch HSR, poiché la sua implementazione potrebbe variare in modo significativo in funzione dell'ambiente. Non va infatti dimenticato che differenti tipi

di schede sono equipaggiate con oscillatori molto diversi da loro; questi ultimi possono essere fissi o regolabili e caratterizzati da valori di accuratezza e range di frequenza molto dissimili tra loro. In questo caso il periodo di clock è necessario per il blocco di commutazione HSR. In funzione dell'implementazione, il periodo di clock può essere fornito anche ai chip PHY corredati di funzionalità IEEE 1588, ai MAC Ethernet e ad altri blocchi che richiedono una temporizzazione accurata, ad esempio per la marcatura temporale (time stamping) delle misure dei valori campione.

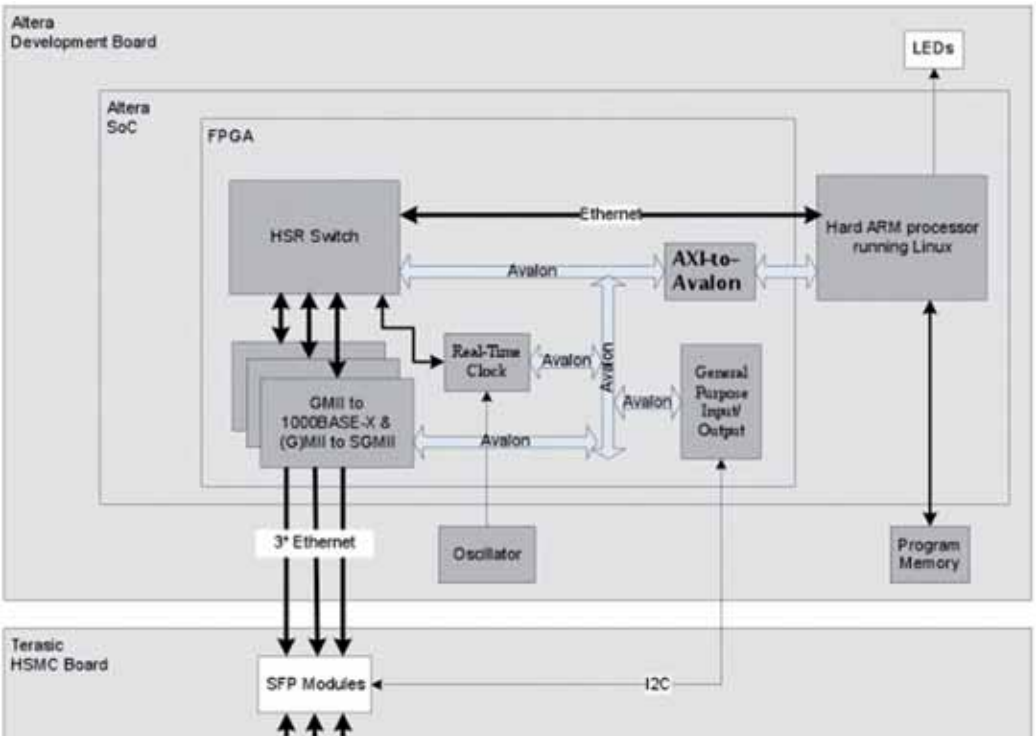


Fig. 2 – Schema a blocchi delle due schede

La struttura di commutazione Avalon collega i blocchi al processore ARM di tipo hard attraverso il bridge AXI-Avalon. Di utilizzo molto comune e basato su uno standard aperto, Avalon rappresenta la scelta ideale per l'implementazione degli accessi ai registri interni dell'FPGA. Il processore esegue il monitoraggio e il controllo delle funzionalità dei blocchi connessi attraverso Avalon mediante l'accesso ai registi di Avalon. Per esempio, esso effettua il monitoraggio in modo continuo della velocità di interfacciamento dei moduli SFP per connessioni in rame, mediante un'interrogazione ciclica (polling) del chip PHY presente all'interno del modulo. Nel momento in cui cambia la modalità, il processore configura in modo appropriato la velocità dell'adattatore (G)MII-SGMII e della porta dello switch HSR.

Implementazione pratica di HSR...

Poiché la topologia tipica di una rete HSR è del tipo ad anello, in generale il numero di salti (hop) tra la sorgente e la destinazione sarà maggiore rispetto a quello delle topologie Ethernet tradizionali. Per questo motivo i requisiti di latenza di inoltro (forward latency) dei dispositivi sono così ridotti da rendere praticamente impossibile l'implementazione di un nodo HSR con un engine di inoltro basato su software. Poiché HSR è una tecnologia relativamente nuova e in continua evoluzione, le realizzazioni sono basate su blocchi IP implementati mediante FPGA. A questo punto val la pena sottolineare che HSR è fondamentalmente basata sui concetti tipici di Ethernet, ragion per cui le reti HSR adottano parecchie tecnologie mutuate dalle tradizionali reti Ethernet, come ad esempio LAN virtuali e assegnazione di priorità. L'implementazione interna di uno switch HSR, con le sue funzionalità di apprendimento degli indirizzi e le code in uscita multiple, è dunque molto simile a quella degli classici switch Ethernet. Un'implementazione HSR, d'altro canto, non può essere solamente di tipo hardware.

A causa della ridondanza, non è possibile individuare singoli guasti della rete senza ricorrere a un protocollo specifico denominato protocollo di supervisione HSR. Quest'ultimo protocollo controlla gli altri nodi della rete HSR, i numeri di sequenza dei loro frame di supervisione e identifica le porte ridondanti che ricevono i frame, memorizzando le informazioni in una tabella denominata tabella dei nodi (nodes table). Queste informazioni possono essere impiegate per localizzare i link non funzionanti correttamente e altri problemi della rete. Per ragioni pratiche, questo protocollo relativamente complesso non può essere implementato in hardware, bensì in software. Vista la necessità di far ricorso a risorse hardware e software per l'implementare di una rete HSR, un SoC permette di realizzare una soluzione HSR sfruttando un unico chip.

IEEE 1588 PTP: informazioni di base

Il protocollo PTP (Precision Time Protocol) definito nello standard IEEE 1588 consente la sincronizzazione del clock per reti Ethernet. Nelle applicazioni in cui il protocollo è in grado di eliminare il ricorso a una rete di sincronizzazione separata è possibile conseguire notevoli benefici economici.
Le implementazioni di una rete IEEE 1588 PTP si differenziano notevolmente in funzione del livello di accuratezza desiderato. La tecnologia di rete riveste un ruolo di fondamentale importanza sull'accuratezza. Le tecnologie DSL sono caratterizzate da livelli di accuratezza nettamente inferiori rispetto a Fast Ethernet, mentre Gigabit Ethernet fornisce risultati nettamente migliori rispetto a Fast Ethernet; in linea generale si può affermare che una maggior capacità corrisponde a una migliore accuratezza. Per quel che concerne la sincronizzazione, la fibra è consigliata rispetto al rame. Le implementazioni IEEE 1588 PTP possono essere di tipo completamente software, ma per sfruttare al meglio le potenzialità offerte da questa tecnologia è necessario utilizzare componenti hardware espressamente ideati per supportare IEEE 1588 PTP.
L'hardware può essere impiegato ad esempio per registrare i tempi esatti di invio e ricezione di determinati frame e in taluni casi (one step clock) modificare i frame "al volo". Utilizzando componenti hardware dedicati è possibile conseguire livelli di accuratezza dell'ordine del nanosecondo quando si utilizza Gigabit Ethernet con cavi in fibra ottica.
IEEE 1588 include un algoritmo di selezione del clock master (Best Master Clock) che in pratica decide quale dei clock presenti nella rete è quello principale e quali invece sono "slave". In questo modo tutti i clock nella rete saranno automaticamente eseguiti contemporaneamente e il sistema è in grado di resistere a malfunzionamenti che coinvolgono il clock e la rete. I clock trasparenti sono clock che permettono di migliorare l'accuratezza della sincronizzazione tra i clock master e slave compensando gli errori provocati dai nodi della rete.
Nelle reti Ethernet, i clock trasparenti sono integrati negli switch Ethernet dove avviene la correzione dell'errore prodotto dai ritardi di accodamento (queuing delay) dello switch mediante la modifica "al volo" dei messaggi PTP coinvolti.
Poiché HSR è solitamente utilizzato nelle medesime applicazioni di IEEE 1588 PTP, le specifiche del protocollo HSR definiscono le modalità di utilizzo di IEEE 1588 PTP con HSR. I frame IEEE 1588 devono essere gestiti in maniera opportuna poiché la rete HSR prevede due o più percorsi funzionali tra i clock mentre le tradizionali reti Ethernet ne hanno solo uno.
Ciò significa ad esempio che non è possibile utilizzare i messaggi di follow-up IEEE 1588 PTP in una rete HSR, poiché il ricevitore non potrà sapere se il messaggio ha viaggiato lungo lo stesso percorso, attraverso la rete, utilizzato dal corrispondente segnale di sincronismo; per tale motivo sarà necessario ricorrere al clock one-step (messaggio di sincronismo senza messaggio di follow-up) invece che clock two-step (messaggio di sincronismo e di follow-up).

... e di IEEE 1588 PTP

Anche nel caso dell'implementazione di IEEE 1588 si fa ricorso a componenti sia hardware sia software. Laddove non vi sono requisiti real-time – algoritmo di selezione del clock master, stack del protocollo, generazione di frame Ethernet e così via – la realizzazione software è senza dubbio la più adeguata. Per quanto concerne invece i task critici dal punto di vista della temporizzazione – acquisizione dei tempi esatti di trasmissione e ricezione, modifica del campo di correzione dei messaggi di sincronismo (Sync), Delay_Req, Pdelay_Req e Pdelay_Resp – con un'implementazione di tipo hardware è possibile ottenere livelli di accuratezza inferiori al microsecondo su reti Ethernet.

A questo punto si tenga presente che con realizzazioni interamente basate sul software è molto difficile ottenere livelli di accuratezza inferiori al millisecondo, mentre con un'implementazione che prevede anche componenti hardware il livello di accuratezza può essere dell'ordine del nanosecondo. Sebbene siano reperibili sul mercato chip per il livello fisico di IEEE 1588, in questo caso non risultano necessari.
La funzionalità di clock trasparente prevista da IEEE 1588 nello switch e quella di marcatura temporale (timestamp) nella connessione switch-HPS elimina la necessità di supportare IEEE 1588 nei chip PHY. In tal modo è possibile ad esempio utilizzare IEEE 1588 PTP con moduli SFP per connessioni in rame prive di supporto per IEEE 1588 PTP.

Reti industriali: a ciascuno il suo protocollo

L'articolo illustra una panoramica dei protocolli di rete industriali e ne descrive le principali applicazioni

Silvano Iacobucci

La comunicazione digitale è uno scambio di dati tra dispositivi elettronici "intelligenti", dotati di appositi circuiti e interfacce. La comunicazione avviene solitamente in forma seriale, cioè i bit che costituiscono un messaggio o un pacchetto di dati sono trasmessi uno dopo l'altro sullo stesso canale di trasmissione (mezzo fisico). Le apparecchiature che devono scambiarsi le informazioni sono connesse tra loro in una rete di comunicazione. Una rete è genericamente composta da nodi interconnessi con linee di comunicazione; il nodo (un dispositivo "intelligente" in grado di dialogare con altri dispositivi) è il punto di trasmissione e/o ricezione dei dati; la linea di comunicazione è l'elemento di connessione di due nodi e rappresenta il percorso diretto che l'informazione segue per essere trasferita tra i due nodi; è in pratica il mezzo fisico (cavo coassiale, doppino telefonico, fibre ottiche, raggi infrarossi) sul quale viaggiano le informazioni e i dati (Fig. 1). Le principali reti di comunicazione possono essere classificate secondo le seguenti topologie: ad anello, a stella, a bus.

Per gestire il traffico dei dati sulla rete e far sì che due dispositivi che dialogano siano in grado di comprendersi a vicenda è necessario un protocollo di comunicazione, un insieme di regole e comportamenti che due entità devono rispettare per scambiare correttamente informazioni tra loro. I protocolli utilizzati per far comunicare i diversi dispositivi nelle applicazioni industriali sono numerosi, e variano in base alle esigenze di comunicazione di ciascuna applicazione, che comprendono: quantità di dati da trasmettere; numero di dispositivi coinvolti; caratteristiche dell'ambiente in cui avviene la comunicazione; vincoli di tempo; criticità dei dati da inviare; correzione degli errori di trasmissione.

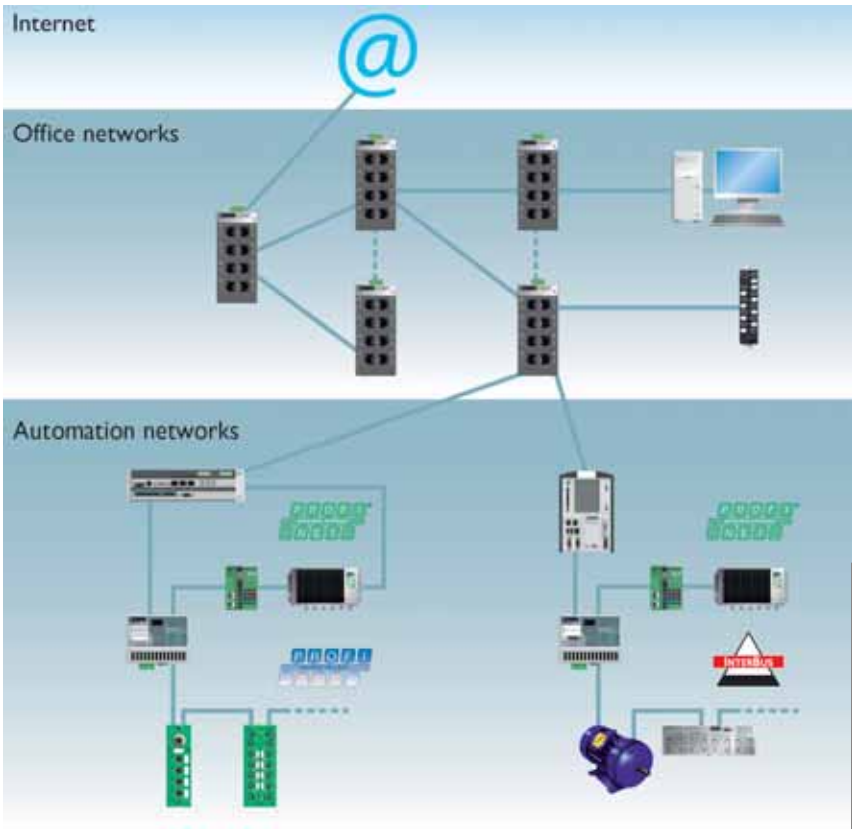


Fig. 1 – Rete di comunicazione process automation

I protocolli attualmente utilizzati nelle comunicazioni industriali sono piuttosto complessi. Per semplificarne la descrizione, si è soliti separarne i livelli di funzionamento distinguendo un livello fisico (physical layer), un livello di collegamento (data link) e un livello applicativo (application layer). In generale i livelli sono indipendenti l'uno dall'altro ma nell'ambito di ciascun livello deve essere adottato lo stesso protocollo da entrambi i nodi per potersi comprendere; per fare un esempio con una

comunicazione tra persone, il livello fisico è rappresentato dal mezzo con cui ci si parla (es. per telefono o con radio ricetrasmittenti), il livello di collegamento è costituito dalla lingua utilizzata (es. inglese o italiano) e il livello applicativo è l'argomento della conversazione.
Il livello fisico specifica il collegamento tra i diversi dispositivi dal punto di vista hardware e descrive i segnali elettrici utilizzati per trasmettere i bit dall'uno all'altro; descrive, ad esempio, i collegamenti elettrici e i metodi di cablaggio, le tensioni e le correnti utilizzate per rappresentare i bit "1" e "0" e le loro durate. Le modalità di collegamento possono essere senza fili (wireless) quando utilizzano come mezzo fisico onde radio, raggi infrarossi o segnali luminosi che si propagano liberamente nello spazio, oppure cablate (wired) in cui i segnali sono trasmessi tramite cavi in rame o fibra ottica, di tipo punto-punto o multipoint, parallelo o seriale. Tra i protocolli di comunicazione più usati si possono citare lo standard IEEE488 per il parallelo e gli standard Rs232C (punto-punto), Rs422 e Rs485 (multipoint) per il seriale. Un altro protocollo comunemente usato con porte Pc seriali è il protocollo HART (Highway Addressable Remote Transducer), basato su una rete ibrida che addiziona un segnale digitale al segnale analogico 4-20 mA e la sua variante WirelessHart.
Il livello di collegamento descrive come i bit sono raggruppati in caratteri e questi ultimi in pacchetti, e come vengono rilevati e corretti eventuali errori. Se necessario, definisce anche i turni o le priorità che i dispositivi devono rispettare per accedere al mezzo di trasmissione. Si parla di protocolli master-slave quando uno dei dispositivi (il master) ha il compito di controllare e gestire la comunicazione di tutti gli altri (slave). Si parla invece di sistemi peer-to-peer quando tale gerarchia non esiste e i dispositivi accedono al mezzo di comunicazione in modo eguale (in tal caso il protocollo comprende le procedure per gestire i turni e le precedenze di accesso al mezzo di comunicazione; ne è un classico esempio Ethernet).
Il livello applicativo descrive quali sono i dati trasmessi e quale è il loro significato relativamente al processo sotto controllo. In altre parole, associa un comando (es: apri/chiudi l'interruttore) o un numero (es. valori di tensione) ai dati in formato binario che i dispositivi si scambiano attraverso la rete di comunicazione. È il livello in cui si specifica quali dati devono essere contenuti nei pacchetti trasmessi e ricevuti e come sono utilizzati.
I metodi di comunicazione punto-punto, largamente usati fin dagli anni '80, si sono integrati ed evoluti negli ultimi decenni nei bus di campo (fieldbus) per ridurre i costi di connettività

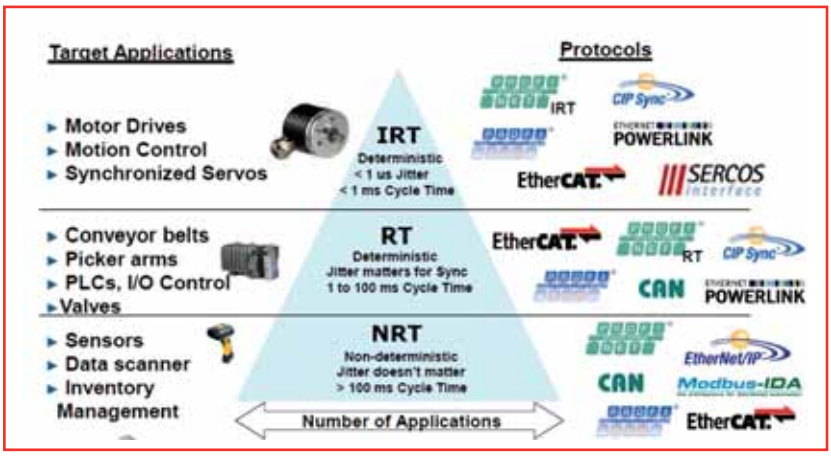
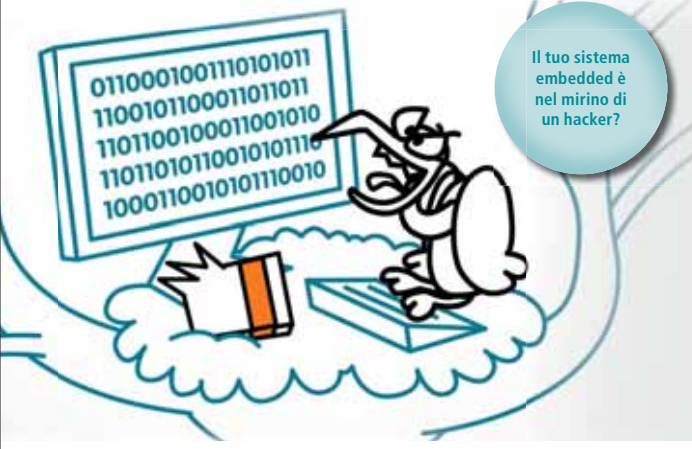


Fig. 2 – Protocolli e applicazioni (fonte Freescale)

PERFECTION IN PROTECTION, LICENSING AND SECURITY

Dai una marcia in più al tuo sistema embedded

WIBU SYSTEMS



- Protezione del know-how e della proprietà intellettuale da
  - reverse-engineering
  - pirateria e contraffazione
- Protezione dell'integrità e degli accessi da
  - manomissioni e intrusioni
- Protezione della documentazione di servizio e dei dati di produzione
- Gestione licenze software dinamica e personalizzabile
- Semplice integrazione in software e processi aziendali in essere

CodeMeter supporta:

Microsoft .NET Framework · Mac · Universal · Java · CODESYS · OPC FOUNDATION

+39 0350667070
sales@wibu.com
www.wibu.it

e ottenere migliore qualità di trasmissione, in reti industriali dove dispositivi intelligenti lavorano in modo cooperativo in modalità distribuita e con tempistiche critiche.
Tra i protocolli di comunicazione più usati (Fig. 2) si possono annoverare: Modbus, protocollo di connessione royalty-free molto diffuso fra i dispositivi elettronico-industriali sviluppato per applicazioni Plc e in grado di interfacciare anche sistemi Scada (Supervisory Control And Data Acquisition); ProfiBus, usato per la comunicazione di campo con sensori e attuatori intelligenti, in genere con scambio dati veloce e ciclico tra apparecchiature di campo e controllori, che nel tempo ha guadagnato un ampio grado di accettazione sia nella produzione sia nell'automazione di processo; DeviceNet, anch'esso usato per l'interfaccia tra dispositivi di campo e controllori (PC, PLC); AS-i, per la comunicazione con sensori molto semplici, come i fine-corsa, o dispositivi di comando (es. pulsanti); Fieldbus Foundation, protocollo di comunicazione aperto e bidirezionale molto usato in automazione di fabbrica e controllo di processo; CAN (Controller Area Network), bus seriale usato tipicamente in ambienti di automazione rumorosi (elettromeccanica) dove l'integrità dei dati deve essere del 100%; LonWorks, protocollo usato in applicazioni di automazione e controllo legate al settore del building automation, come ad esempio l'illuminazione e i sistemi di condizionamento ambientale; Interbus, che ha il vantaggio di permettere il collegamento tra due dispositivi posizionati a distanze fino a 500 m con un cavo standard, senza perdere prestazioni in termini di velocità e mantenendo stabilità e garanzia dei dati. L'interfaccia Sercos (Serial real-time Communication System) fornisce un sistema di comunicazione standard, real-time, ad alte prestazioni tra controllori di movimento, servo drive digitali e dispositivi di input/output (I/O).
È un protocollo ideale per applicazioni dove la gestione accurata di coordinate di movimento su assi multipli è un fattore critico. Sercos è registrato come standard IEC 61491.
La maggior parte dei fieldbus si è ulteriormente evoluta negli ultimi anni, per rispondere alle esigenze di interoperabilità e di elevate prestazioni richieste dal mercato, integrandosi con il protocollo Ethernet e dando origine a corrispondenti protocolli denominati "Industrial Ethernet".
Tra questi si possono elencare in particolare i protocolli Profinet (la versione Ethernet based di Profibus), Ethernet/IP (evoluzione di DeviceNet), Ethernet Powerlink (evoluzione di CANOpen) e Modbus-TCP (versione Ethernet di Modbus-RTU).

Fig. 3 – Sistema Axioline (Phoenix Contact)

Applicazioni e soluzioni

Dopo una carrellata veloce sui principali protocolli, si analizzano le loro principali applicazioni con il supporto di due fornitori presenti sul mercato italiano: Phoenix Contact e Ifm Electronic.
Nel settore dell'automazione di processo la parola d'ordine è "sicurezza". Il bus di campo è sempre diffuso grazie soprattutto alla facilità di realizzazione della rete, alla diagnostica integrata e alla conseguente riduzione dei costi di cablaggio. Gli standard a più ampia diffusione sono quelli che meglio incontrano le esigenze correlate all'ambiente critico tipico dell'industria di processo, caratterizzato da un elevato rischio di esplosioni o incendi e pertanto necessitante di dispositivi adeguati agli stringenti requisiti SIL che regolano gli impianti per garantirne la sicurezza. In questo settore, inoltre, vi è spesso l'esigenza di rendere disponibile l'alimentazione tramite il cavo di rete, anche su distanze di centinaia di metri, e di coprire contemporaneamente applicazioni di fabbrica discrete (ad esempio pompe, trasportatori, attuatori e sistemi robotizzati) e di processo (come trasmettitori di pressione e temperatura); nella maggior parte degli impianti, infatti, gli strumenti legati a questi due tipi di funzioni lavorano a fianco gli uni agli altri, cosicché avere un bus di campo unico per entrambi comporta un notevole risparmio sui costi. All'interno di questo settore specifico vengono dunque utilizzati principalmente bus di campo quali Fieldbus Foundation e Profibus PA.
Come nei restanti settori industriali, inoltre, anche nel processo la comunicazione wireless sta diventando sempre più diffusa e importante. Partendo da questo presupposto HART Versione 7 definisce il wireless come la nuova tecnologia di trasferimento dati per l'automazione di processo, con WirelessHART.
Nel settore dell'industrial manufacturing si prediligono invece integrazione e rapidità. Dai costruttori di macchine e dalla relativa filiera giungono quotidianamente richieste di applicazioni e soluzioni relative a bus di campo tradizionali e sistemi innovativi basati sul trasferimento di informazioni in industrial Ethernet.
Infatti le esigenze comuni di questo settore comprendono la costante ricerca di razionalizzazione dei cablaggi, la riduzione degli ingombri occupati dalle macchine stesse, la versatilità di comunicazione tra parti di macchine e sistemi ERP di livello superiore. Nella proposta di bus di campo attuali e di nuova generazione diviene dunque fondamentale fornire loro proposte sempre più performanti, compatte e di design ricercato oltre che architetture sempre più integrabili. In questo ambito sono

dunque protocolli come Profinet e Interbus a farla da padrone. Grazie alla sua totale integrazione nella rete Ethernet standard, Profinet permette di implementare reti Ethernet sia di tipo office sia industriali e di collegare dispositivi capaci di supportare tutti i mezzi di trasmissioni standard. Dal canto suo, invece, Interbus (sviluppato da Phoenix Contact e standardizzato EN 50254 e IEC 61158) offre il massimo delle prestazioni in linee e impianti rimanendo immune a disturbi EMC anche su distanze lunghe. Profinet, con la versione IRT, presenta una modalità di trasmissione dei pacchetti dati molto simile a quella utilizzata dal protocollo Interbus, dove i messaggi vengono compattati e scompattati direttamente nello switch, con il risultato che il dispositivo interessato riceve solo le informazioni necessarie, guadagnando in efficacia ed efficienza.

Fig. 4a – Controllore ad alte prestazioni RFC 460R PN 3TX di Phoenix Contact

Più varia la situazione riscontrabile nell'ambito del mercato "Infrastructure", in cui si collocano varie realtà, anche molto diverse tra loro - come il ferroviario, il trattamento delle acque e la produzione e distribuzione delle energie da fonti alternative. Di conseguenza, anche i sistemi presenti in questo campo sono svariati: CANopen rappresenta ad esempio lo standard per tutti i sottosistemi presenti negli aerogeneratori, mentre Modbus, grazie alla sua semplicità e alla sua posizione di standard in ambito industriale, trova ampio impiego, nelle versioni RTU e TCP, rispettivamente per la comunicazione con la strumentazione installata in campo (sensori evoluti, centraline di raccolta dati, I/O remoti) e lo scambio di dati su rete Ethernet ad alta velocità (100 Mbit/s), sia che si tratti di controllo negli aerogeneratori o di applicazioni per il telecontrollo e la telegestione.
Un'esigenza comune a una grande parte di queste applicazioni è però quella di trasmettere dati in modo affidabile a elevata distanza, anche in situazioni tali da rendere problematica la realizzazione di reti cablate. Di conseguenza, anche in questo settore trovano ampio spazio le infrastrutture di comunicazione wireless.

Prodotti disponibili: alcuni esempi

Phoenix Contact è attenta a fornire ai vari settori di utilizzatori le soluzioni più idonee, a partire dai protocolli di rete e dagli strumenti di comunicazione.
Nel settore process automation ad esempio propone accoppiatori di segmento per fieldbus FB-2SP e FB-ISO, che permettono di collegare i dispositivi in campo con una soluzione modulare partendo dall'alimentatore per Fieldbus Foundation e Profibus PA invece che essere legati all'adozione di moduli con numero di canali fisso (4, 8, 12). Per le reti WirelessHART Phoenix Contact offre un gateway dotato di transceiver WLAN integrato a norma IEEE 802.11b/g. Il dispositivo, che può essere montato su una guida DIN ed è alloggiato in una custodia IP20, collega fino a 250 moduli di campo WirelessHART ed è costituito da un access point WirelessHART, un network manager e un'interfaccia Gateway con WLAN Client. Converte automaticamen-

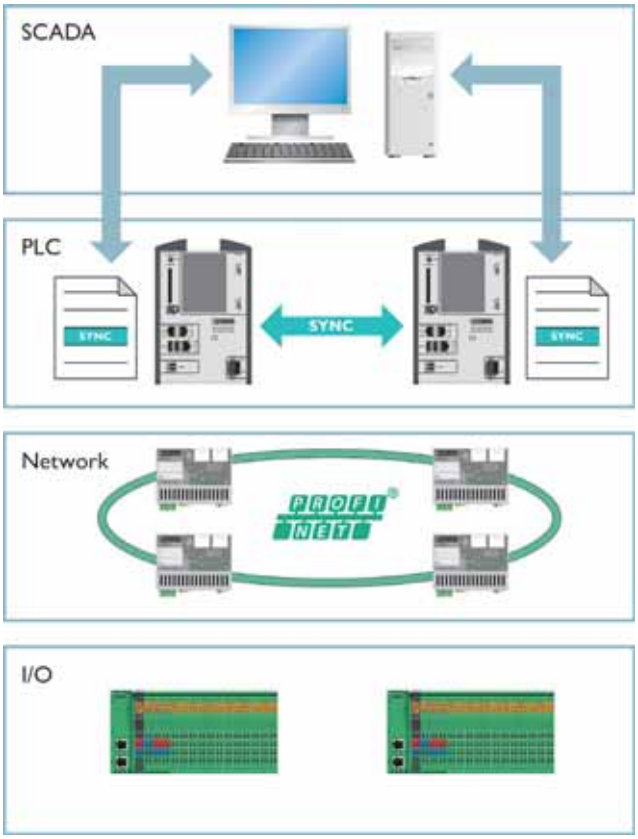


Fig. 4b – Modalità di utilizzo del controllore RFC 460R PN 3TX in rete

te i dati HART in Modbus/TCP, in modo tale che i moduli di campo possano essere facilmente integrati in quasi tutti i sistemi di controllo. La codifica dei dati WLAN con lo standard IEEE-802.11i (WPA2 - Wi-Fi Protected Access 2) e con un AES (Advanced Encryption Standard) a 128 bit garantisce un collegamento backhaul sicuro. Opzionalmente, è possibile disattivare il transceiver WLAN e collegare l'host mediante Ethernet via cavo a 10/100 MBit/s.
Nel settore industrial manufacturing, Phoenix Contact offre modem industriali per tutte le interfacce, capaci di garantire la possibilità di effettuare un accesso remoto ottimale per un'efficace manutenzione a distanza, un'acquisizione dati continua e una segnalazione di allarme. I nuovi modem, per linea dedicata DSL, permettono velocità di trasmissione fino a 30 MBit/s anche su cavi in rame già esistenti. Inoltre la società propone il sistema di I/O real-time Axioline (Fig. 3) per montaggio nel quadro elettrico. Grazie a un offset di un solo µs per modulo, con Axioline la velocità del sistema è definita dalla rete di livello superiore. Supporta i protocolli di comunicazione basati su Ethernet ed è ottimizzato per Profinet. Questo sistema amplia la gamma di moduli I/O di Phoenix Contact, affiancando la gamma Inline (per montaggio ad interno quadro) e Fieldline (per installazione a bordo macchina). Grazie al router/switch FL NAT SMN 8TX, per semplificare la configurazione personalizzata dei singoli terminali Ethernet i costruttori di macchine possono godere dei numerosi vantaggi offerti dall'impiego del routing o 1:1-NAT (Network Adress Translation). In questo modo un host esterno può raggiungere l'apparecchio interno, come se entrambi fossero installati nella stessa sottorete.
Nel settore infrastructure la gamma di prodotti Phoenix Contact include PLC compatti con eccellenti funzioni di comunicazione, ideali per diverse applicazioni di automazione come il modello RFC 460R PN 3TX (Figg. 4a e 4b). Grazie al software PC Worx Express, per i PLC è disponibile un ambiente di sviluppo gratuito. Tutti i PLC sono provvisti di almeno una porta Ethernet, dispongono di server web e FTP integrati, supportano diversi protocolli di comunicazione (tra cui SNMP e Modbus TCP) e possono interfacciarsi direttamente a database SQL. La gamma è composta da ILC 130 ETH (entry level), ILC 150 ETH, ILC 150 GSM/GPRS (con modem GSM/GPRS integrato), ILC 170 ETH 2TX (con due porte Ethernet, memoria estraibile in formato SD e supporto funzionalità Profinet IO Device) e dall'ultimo nato, ILC 190 ETH 2TX; questo PLC, oltre ad avere le caratteristiche di ILC 170 ETH 2TX, ha una memoria per programmi pari a 1 MB e integra un'unità floating point (FPU). Grazie alla possibilità di affiancare i moduli I/O del sistema di automazione Inline, le possibili applicazioni sono praticamente illimitate e, con la tecnologia SafetyBridge, è possibile realizzare soluzioni di sicurezza funzionale distribuite senza dovere ricorrere a un PLC di sicurezza. Il nuovo Ethernet Port Adapter FL WLAN EPA di Phoenix Contact consente di integrare dispositivi di automazione in reti wireless WLAN 802.11b/g in modo sicuro, semplice e affidabile. L'adattatore viene connesso direttamente alla porta Ethernet del dispositivo di automazione come client WLAN industriale. La possibilità da parte di un controllore di accedere a tutte le funzioni WLAN mediante Ethernet, assicura la massima flessibilità nell'implementazione delle applicazioni. Il collegamento con il dispositivo di automazione avviene mediante un normale cavo Ethernet. È inoltre possibile trasmettere protocolli Industrial Ethernet quali Profinet, Modbus/TCP o Ethernet/IP.

Fig. 5 – Sistema IO-Link (IFM Electronic)

Ifm Electronic offre una vasta gamma di sensori IO-Link (Fig. 5) per pressione, livello, temperatura, flusso e AS-i. IO-Link è un'interfaccia di comunicazione punto-punto per sensori e azionatori, indipendente dal costruttore e dal bus di campo utilizzato.
Usufruisce dello stesso cavo dei sensori standard ed è in grado di trasmettere segnali digitali e analogici. Il sistema riunisce le funzioni di parametrizzazione e di diagnosi. Per l'utente si tratta di un sistema plug and play. Se un sensore subisce un guasto, un operatore anche non qualificato può subito sostituirlo con un sensore identico senza ulteriore regolazione. Per il costruttore, la documentazione tecnica è ridotta grazie al salvataggio dei parametri. La configurazione può essere ripetuta facilmente su vari sensori. Inoltre la parametrizzazione e la diagnosi possono essere effettuate a distanza grazie alla tecnologia FDT / DTM a tutti i livelli (sensore, modulo, gateway e PLC).

Sistemi embedded multi-core

La migrazione verso dispositivi multi-core richiede modifiche complesse sia all'hardware sia al software per ottenere prestazioni ottimali. È ragionevole chiedersi se i sistemi multi-core valgano di più o se sia possibile continuare a ottenere miglioramenti attraverso i dispositivi single-core

Maurizio Di Paolo Emilio

Prima dell'avvento dei multicore, gran parte degli sforzi per migliorare le prestazioni era concentrata sulla frequenza di clock ma è diventato fin troppo evidente che spingere la frequenza ha comportato dei costi. I miglioramenti in frequenza penalizzano il consumo di energia, che a sua volta genera calore che richiede più raffreddamento, diminuisce l'affidabilità e riduce la durata del dispositivo.
Una regola è che raddoppiando la frequenza si quadruplica il consumo di energia, che in sè è solo proporzionale alla frequenza e valori superiori hanno bisogno di un aumento di tensione, a causa di processori con transistor più veloci: *Potenza = Capacità * Tensione2 * Frequenza*.
Quindi, raddoppiando semplicemente la frequenza di core non si incrementano proporzionalmente le prestazioni.
Tecniche quali le istruzioni di parallelizzazione e pipelining non possono generalmente scalare con la frequenza. Ad esempio, le pipeline hanno requisiti di temporizzazione interni che non possono essere soddisfatti se si aumenta la frequenza di clock del processore. Pertanto, la latenza di molte istruzioni non può scalare proporzionalmente e sono quindi necessari stadi di pipeline aggiuntivi. Il risparmio energetico è particolarmente critico per i sistemi embedded. In un'implementazione relativa a un sistema convenzionale, il massimale standard di circa 20-40W richiede un dissipatore di calore e un ventilatore o un notevole flusso d'aria per il raffreddamento. Garantire che i punti caldi siano distribuiti complica efficacemente sia il layout della scheda, sia la disposizione delle schede all'interno di un sistema più grande.
Questo può essere accettabile per i dispositivi di fascia alta, ma non quando i requisiti di alimentazione scendono al di sotto di circa 7W.
Esistono dispositivi multi-core a bassa potenza che consumano solo circa 2W, come MPC5121 basato su E300 con grafica integrata e un acceleratore di elaborazione del segnale.

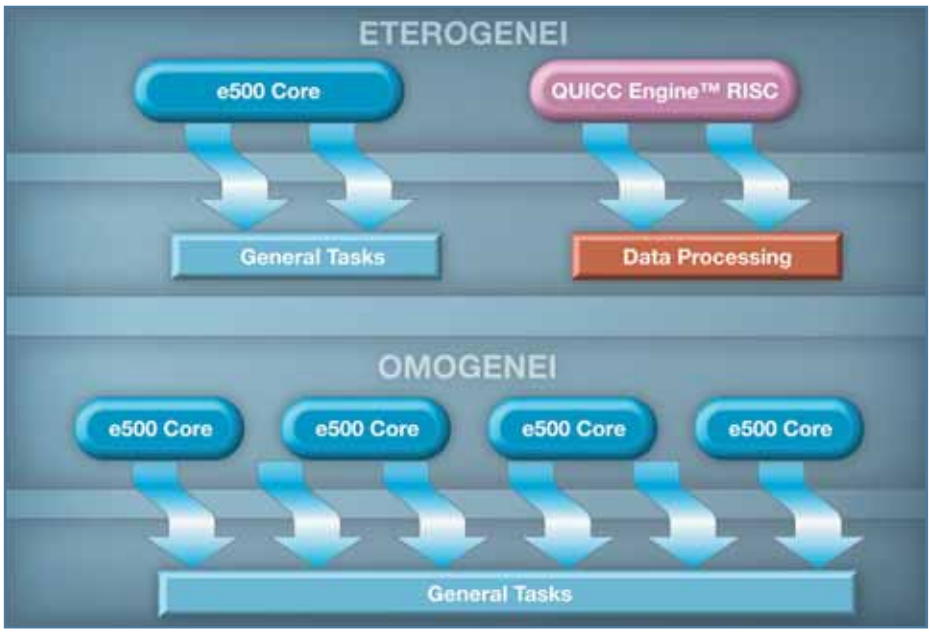


Fig. 1 – Ambienti multicore

asPer la maggior parte delle applicazioni, questi dispositivi possono essere attuati senza dissipatore.
Tra i vantaggi dei multicore si ha una possibile utilizzazione del clock a frequenze maggiori, un uso più efficiente delle memorie cache, dei tempi di risposta migliori con carichi di lavoro intensi, una notevole riduzione del PCB per lavorare con correnti più basse, quindi meno dispersione di calore. Per far ciò sono necessarie modifiche al sistema operativo e ai programmi e in generale sono più difficili da gestire rispetto ai sistemi monoprocessori.

Tipi di multi-core

Data la crescente importanza del multiprocessing, tutto lo spettro di calcolo e i sistemi di fascia alta, quali le infrastrutture di telecomunicazione, server e supercomputer, hanno a lungo utilizzato design multi-core come standard.
Dispositivi multicore sono stati utilizzati in diverse forme per molti anni, come ad esempio i dispositivi PowerQUICCTM Freescale, costruiti sulla tecnologia Power ArchitectureTM, come i core e500 utilizzati nei dispositivi PowerQUICC III e core singolo o doppio RISC nella unità di comunicazione QUICC EngineTM.
La figura 1 mostra diversi tipi di ambienti multicore per Freescale Semiconductor. Un dispositivo che contiene più core con diversi tipi di set di istruzioni viene indicato come eterogeneo; in contrasto, dispositivi multicore omogenei implementano più core identici, come nel MPC8641 e P2020.

La figura 2, invece, mostra topologie di memoria di base in riferimento sempre a Freescale Semiconductor:

- nei design a memoria distribuita, ogni CPU ha tipicamente una memoria privata e la comunicazione tra le CPU avviene tramite una rete ad alta velocità;
- in un progetto a memoria condivisa, c'è una memoria pubblica che è condivisa da più core;
- in un design ibrido, vi è una risorsa di memoria condivisa ma ogni core ha una memoria privata.

Questo permette ad ogni CPU/core di avere una memoria privata che può essere agevolmente condivisa su una memoria pubblica.

Come la tecnologia di processo si restringe sotto i 45 nm, i dispositivi possono essere realizzati non solo con due e quattro core, ma con molte decine di core, un approccio comunemente indicato come many-core piuttosto che multicore. Un dispositivo dual-core in genere può fornire un aumento delle prestazioni senza alcuna modifica, poiché il sistema operativo può dedicare un core per l'applicazione principale e l'altro per compiti particolari quali la gestione di interrupt.

Parallelismo

La parallelizzazione è la sfida centrale nello sviluppo di un ambiente multicore e può essere pensata con quattro livelli

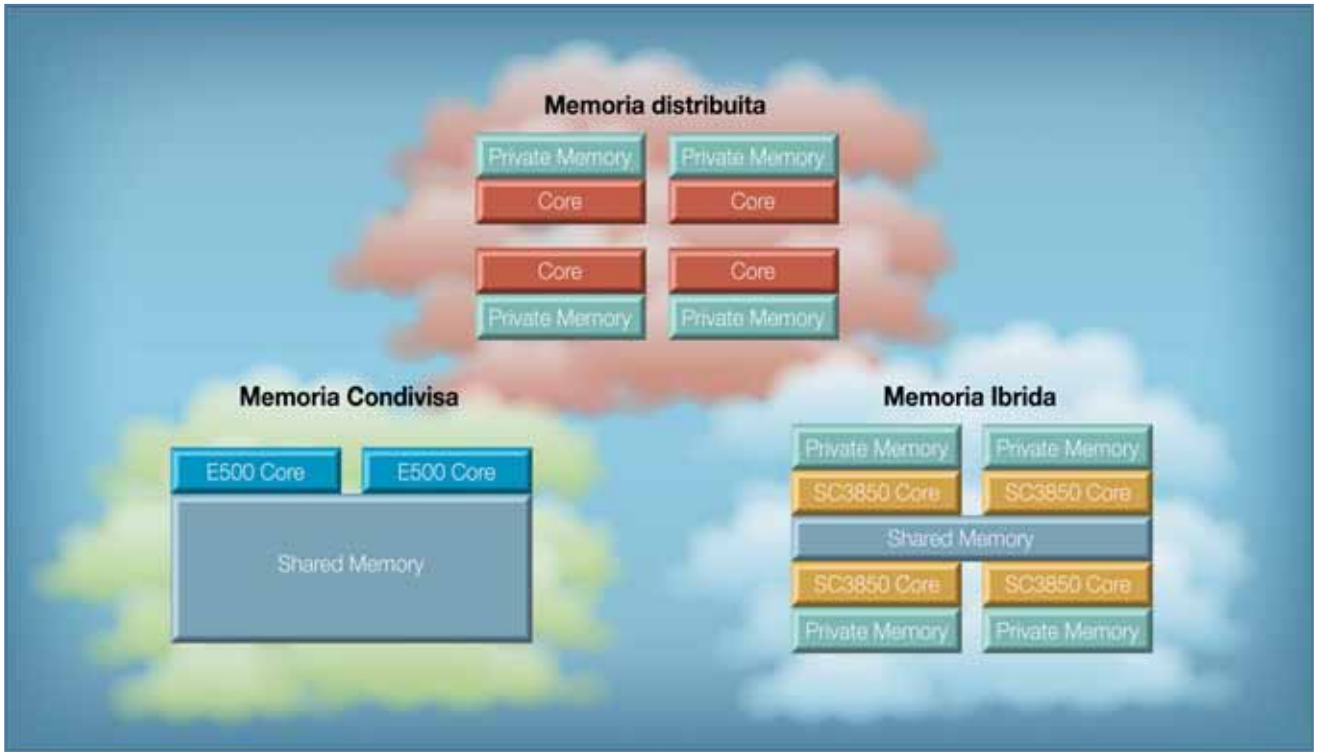


Fig. 2 – Design di memoria in sistemi multi-core

fondamentali: bit level, instruction, data, e task. Bit level estende l'architettura hardware per operare contemporaneamente su dati più grandi. Ad esempio, su un core a 8-bit, il calcolo su un oggetto dati a 16 bit richiede due istruzioni. Istruzione di parallelismo (ILP, instruction) è la tecnica per identificare istruzioni che non dipendono l'una dall'altra. Poiché i programmi sono in genere sequenziali in struttura, questo non è un compito facile e alcune applicazioni, come l'elaborazione del segnale per voce e video, possono funzionare in modo efficiente. Parallelismo dei dati (data) consente a più unità di elaborare i dati contemporaneamente. Una di queste tecniche è implementata in hardware SIMD (Single Instruction/multipli di dati), e viene realizzata nelle istruzioni di vettore a 128-bit, definite dal set di istruzioni AltiVec e le istruzioni vettoriali a 64 bit. Task di parallelismo distribuisce diverse applicazioni, processi o thread a diverse unità. Questo può essere fatto manualmente o con l'ausilio del sistema operativo.

Software design

Il modo più semplice per passare da single-core a multicore computing è di eseguire ogni core in modo indipendente. Questo approccio è chiamato multiprocessing asimmetrico (AMP o ASMP) in contrasto con SMP (SMP).
In un design AMP, ogni core è dedicato a una singola attività, come decodifica dati in entrata o manipolazione di essi. Questo può essere fatto in un core polivalente o in core progettati su misura che hanno una unità di sicurezza dedicata per eseguire la crittografia e la decrittografia, come P2020 di Freescale.
Con i sistemi AMP, è importante che l'hardware distribuisca il lavoro tra i core. Nel caso di traffico Ethernet, per esempio, questo può essere fatto mediante filtraggio di indirizzi MAC o IP per core specifici. Tuttavia, con un design SMP, si richiedono core omogenei che condividono memoria in modo tale che qualsiasi processo possa essere assegnato a qualsiasi core in qualsiasi momento. Supponendo che un'applicazione sia divisa in più thread, questo è un approccio molto conveniente, poiché il sistema operativo svolge la maggior parte del lavoro. Tuttavia si verificano perdite di prestazioni, perché tutti i core competono per la stessa memoria. Combinazioni di SMP e AMP producono buoni risultati in applicazioni come telecomunicazioni 3G/LTE.

Hardware design

Un obiettivo di progettazione hardware è quello di minimizzare il consumo energetico reso possibile dalla migrazione a sistemi multicore. I dispositivi di solito implementano i modi che fermano l'esecuzione o spengono il dispositivo per diversi gradi. Tuttavia queste modalità possono essere difficili da attivare nel software, e la riattivazione può richiedere molto tempo, specialmente se i PLL (phase-lock loop) richiedono risincronizzazione. Per semplificare questa operazione vengono introdotte nuove tecniche che interrompono l'esecuzione su un core specifico, finché non si verifica un interrupt.
I dispositivi utilizzano in genere un approccio basato su bus per la comunicazione interna, semplici da progettare e con un'elevata capacità di trasmissione a bassa latenza. Tuttavia, dispositivi multicore devono affrontare due grandi ostacoli: il numero di unità aumenta, così come la lunghezza fisica della connessione al bus.
La soluzione, mostrata in figura 3 consente accessi multipli simultanei. Con tale approccio, come un core comunica con l'interfaccia Serial RapidIO, un altro può accedere alla memoria, un terzo può utilizzare l'interfaccia Ethernet, e così via.

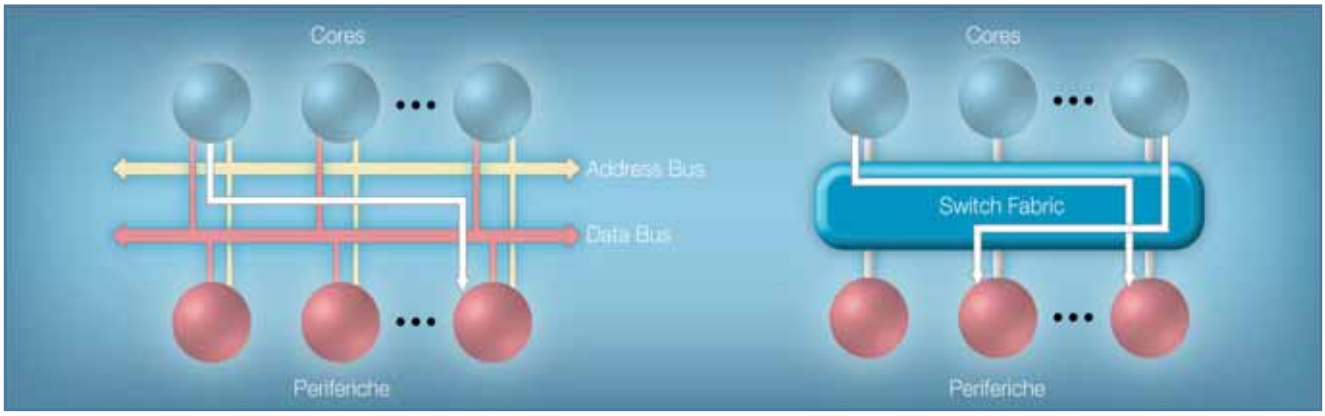


Fig. 3 – Approccio multi-core per bus

Computer industriali

Cresce la varietà delle applicazioni dove occorrono computer rugged capaci di massimizzarne l'utilizzabilità e perciò molti costruttori oggi li propongono un po' dappertutto

Lucio Pellizzari

I computer modulari con caratteristiche di estrema robustezza sono nati per le applicazioni militari e per l'industria ma oggi sono sempre più richiesti in una crescente gamma di applicazioni come, per esempio, il controllo dei sistemi di guida automatizzati delle metropolitane oppure il comando dei sistemi di bordo dei camion. Certamente i computer rugged richiedono metodologie di progettazione molto più rigorose rispetto a quelle dei computer consumer dato che devono trovarsi a sopportare forti vibrazioni meccaniche, ampie variazioni termiche e insidiose radiazioni elettromagnetiche, ragion per cui ci vuole molto più tempo al progettista per scegliere i componenti adeguati e per fare attenzione persino alle tecniche di saldatura dei chip sugli zoccoli.
D'altra parte, la crescente domanda di sistemi rugged ne ha moltiplicato l'interesse del mercato e ciò è servito almeno in parte ad ammansirne i costi di sviluppo oltre che a indurre i costruttori ad aumentare la propria offerta di computer di questo tipo. Oggi per fortuna se ne trovano con un'ampia gamma di funzionalità standardizzate, alle quali si possono aggiungere moduli custom con maggior semplicità rispetto a qualche anno fa, quando bisognava necessariamente ricorrere a progetti ad hoc dai costi spropositati. Inoltre, le nuove interfacce seriali ad alta velocità hanno aggiunto ai computer industriali quella versatilità che ne consente, per esempio, il controllo in rete con la possibilità di ricorrere a moduli ridondanti capaci di sopperire e risolvere istantaneamente qualsiasi problema possa ingenerarsi e favorire così l'utilizzabilità senza interruzioni che è uno dei requisiti fondamentali di questi prodotti.

Aaeon ha introdotto il nuovo computer embedded fanless AEC-6523 specificatamente progettato per le applicazioni con escursioni di temperatura estreme. A bordo si trovano un processore Intel Atom N2600 Dual Core con clock di 1,6 GHz affiancato dall'Intel NM10 Express Chipset e dall'Intel GMA3600 Integrated Graphic Engine, nonché da una memoria base DDR3 di 2 GByte. Nella dotazione ci sono anche quattro porte USB 2.0, due Gigabit Ethernet, un HDD Sata da 2,5", uno slot per CFast Card e quattro seria-

Fig. 1 – Pesa 2,2 kg il computer fanless Aaeon AEC-6523 con operatività termica che va da -40 a +70 °C e resistenza agli urti fino a 50g

li RS-232. L'alimentazione è ammessa da 9 a 30 Vdc mentre il robusto contenitore dal peso totale di 2,2 kg garantisce una tolleranza termica operativa che va da -40 a +70 °C con un'immunità agli urti fino a 50g e alle vibrazioni fino a 5g.

Adlink Technology ha presentato il computer fanless a basso consumo cPCI-3620, progettato per il controllo delle reti ferroviarie. Il formato è 3U e a bordo c'è un processore Intel Atom quad-core E3845 con clock

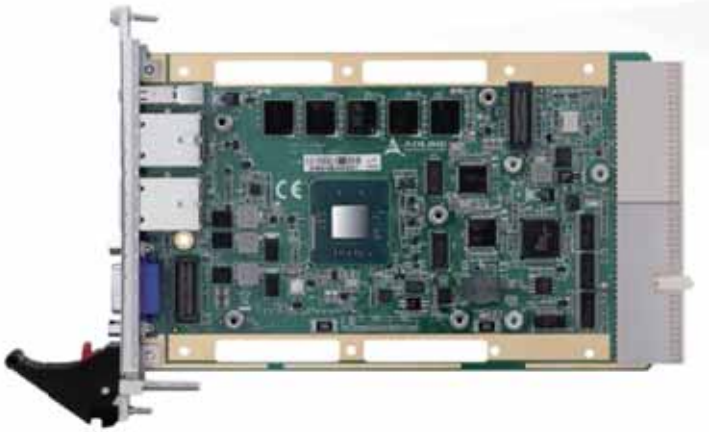


Fig. 2 – Il computer fanless Adlink cPCI-3620 pensato per le applicazioni ferroviarie di Automatic Train Control limita il consumo a 10 W

di 1,9 GHz, che permette di contenere il consumo nelle più impegnative condizioni d'impiego entro 10W. Nella dotazione ci sono anche 4 GByte di memoria DDR3L-1333, un disco allo stato solido da 32 GByte, una USB 3.0, due USB 2.0 e due Gigabit Ethernet. La robustezza è attestata dalla certificazione EN50155 e ne consente l'uso nei sistemi di Automatic Train Control (ATC), dove può sfruttare i moduli pre-installati per il controllo della velocità in curva, dell'efficienza dell'impianto frenante e del corretto funzionamento dei sistemi di guida. La tolleranza termica operativa va da -40 a +75 °C e c'è anche lo Smart Embedded Management Agent (SEMA) per il monitoraggio delle funzionalità di bordo.

Contradata presenta i computer fanless DC-1100 prodotti dalla giovane società taiwanese Cincoze, che li ha progettati pensando alle esigenze del mercato industriale. Il processore è il quad-core Intel Atom E3845, con clock di 1,91 GHz integrato insieme a 4 GByte di memoria DDR3L, mentre nella dotazione

Fig. 3 – Grazie al robusto involucro di alluminio, pesa solo 1,58 kg il computer fanless Cincoze DC-1100 distribuito da Contradata e ammette l'alimentazione da 9 fino a 48 Vdc

si trovano due slot di espansione Mini PCIe, due Gigabit Ethernet, una porta DVI, una DisplayPort, un disco HDD SATA da 2,5", una USB 3.0, tre USB 2.0 e quattro seriali RS232/422/485. Le dimensioni sono di 185x131x54 mm con un peso limitato a solo 1,58 kg da un involucro di robustissimo alluminio, mentre l'alimentazione è ammessa da 9 a 48 Vdc con tolleranza termica da -20 a +70 °C e resistenza all'umidità dal 10% al 95%.

Eurolink Systems introduce l'evoluto eInstrument-PC, ideato da Innovative Integration, una sussidiaria di Interconnect Systems, che progetta e produce sistemi embedded soprattutto basati su DSP e Fpga, ma anche specifici per l'acquisizione dati. L'eInstruments-PC è definito con lo slogan "The Soul of your New Machine" o "l'anima della

Fig. 4 – eInstrument-PC di Innovative Integration è proposto da Eurolink Systems con lo slogan "The Soul of your New Machine" perché totalmente configurabile

vostra nuova macchina" perché è completamente personalizzabile e consente di scegliere la scheda madre COM Express, la CPU Intel Atom i7, la quantità di memoria e la dotazione di periferiche fra cui una Gigabit Ethernet, fino a sei USB 2.0 e uno slot PCIe, da cui può trasferire dati su cavo alla velocità di 200 MByte/s fino a una tratta di 10 metri. Il contenitore misura 250x170 mm e può essere alimentato da 9 a 18 Vdc con un consumo massimo limitato a 6W.

GE Intelligent Platforms ha introdotto la famiglia dei computer industriali fanless a elevate prestazioni RXi Box, per il controllo in tempo reale delle applicazioni embedded negli ambienti critici. Come processore si può scegliere fra l'Intel Atom i7 Dual Core con clock fino a 2,5 GHz, l'i7 Quad Core con clock fino a 2,1 GHz e l'Intel Celeron, tutti con memoria base DDR3L di 4 GByte espandibile a 8 GByte, mentre la tolleranza termica base va da

Fig. 5 – La famiglia dei computer RXi Box di GE Intelligent Platform può essere configurata in diversi modi e adattarsi a un'ampia gamma di applicazioni di controllo in tempo reale

-25 a +65 °C e nella versione estesa da -40 a +85 °C. Modulare ed espandibile, questo computer misura 182x233x98 mm, ospita tre porte Gigabit Ethernet e uno slot PCI Express ed è ideale per l'acquisizione dati nei sistemi di automazione industriale e nei sistemi di controllo automotive a bordo di treni e aerei.

Goma Elettronica propone il computer fanless MXC-2300 di Adlink Technology, basato sul processore Intel Atom quad-core E3845 da 1,91 GHz

Fig. 6 – Goma Elettronica consiglia per le condizioni d'impiego con urti fino a 50g il computer fanless Adlink MXC-2300 con operatività termica da -20 fino a +70 °C

con nome in codice Bay Trail, accompagnato con 4 GByte di memoria DDR3L espandibile fino a 8 GByte. Progettato in forma modulare, questo computer misura 142x219x210 mm, sopporta gli urti fino a 50g e ha una tolleranza termica estesa da -20 fino a +70 °C.
La dotazione presenta una porta USB 3.0, quattro USB 2.0, due Gigabit Ethernet, una DisplayPort, una DVI-I, due CANbus e 16 I/O digitali, mentre per gli slot di espansione si può scegliere fra due PCI e una PCIe x4 oppure tre PCI. L'alimentazione è ammessa da 9 fino a 32 Vdc per consentirne l'uso automotive, mentre il consumo è limitato a 10W anche nelle più severe condizioni d'impiego.

MPL la scorsa estate ha introdotto il computer fanless New Generation CEC che misura 62x162x118 mm e offre una tolleranza termica operativa che va da -40 a +85 °C.
A bordo si può scegliere uno qualsiasi dei processori Intel Atom E3800 a singolo, doppio o quadruplo core, mentre la dotazione prevede cinque porte Gigabit Ethernet, quattro USB, una DisplayPort, una RS232, uno slot mPCIe e due PCIe, ma si possono aggiungere in opzione anche altre interfacce. L'alimentazione è consentita da 8 fino a 36 Vdc e il consumo viene limitato da 8W fino a un massimo di 18W nelle condizioni più impegnative.

Fig. 7 – Misura 62x162x118 mm il nuovo computer rugged interamente progettato e prodotto in Svizzera da MPL e offre un'operatività termica che va da -40 fino a +85 °C

Sistemi Avanzati Elettronici propone l'innovativa famiglia di computer industriali fanless Nuvo-3100VTC/3120 prodotta dalla giovane società Neousys Technology, specializzata nei computer rugged. Le dimensioni del Nuvo-3100VTC sono compatte con uno chassis di soli 210x165x59 mm

Fig. 8 – I nuovi computer Sisav Nuvo-3100VTC/3120 hanno tolleranza termica estesa da -25 fino a +70 °C e si possono alimentare da 8 fino a 35 Vdc

mentre la tolleranza termica operativa si estende da -25 fino a +70 °C con un'immunità agli urti fino a 50g e alle vibrazioni fino a 5g. Il processore è un Intel Atom i7/i5 PGA e nella dotazione si trovano quattro porte Gigabit Power-over-Ethernet 802.3at da 25,5 Watt e due dischi HDD SATA da 2,5" di cui uno hot-swappable.
L'alimentazione è ammessa da 8 fino a 35 Vdc e ne consente l'uso automotive a bordo di treni e camion, nonché nei sistemi di videosorveglianza o nella robotica. Il modello 3120 misura 212x165x62 mm e al posto delle quattro Gigabit PoE ha due porte Gigabit Ethernet, ma entrambi hanno anche quattro porte USB3, una DVI/VGA e uno slot di espansione PCI Express.

Syslogic Group Switzerland è specializzata nella progettazione e produzione in proprio di sistemi per l'automazione industriale con elevati standard

Fig. 9 – Consuma al massimo 10 W il computer fanless Syslogic Compact SL Series con processore Intel Atom E3800 Bay Trail al clock di 1,91 GHz

di qualità e robustezza. Il nuovo computer embedded Compact SL Series si basa sul processore Intel Atom E3800 Bay Trail, che si può scegliere con clock da 1,33 fino a 1,91 GHz e in funzione delle condizioni di impiego garantisce di contenere i consumi da 5 fino al massimo di 10W.
A fianco della CPU si possono mettere fino a 8 GByte di memoria DDR2 e, inoltre, in dotazione ci sono anche tre porte USB 2.0, una USB 3.0, due Gigabit Ethernet, una DVI, una CFast Card, due seriali RS-232, una RS422/485, uno slot di espansione miniPCIe e uno PC/104. Le sue misure sono di 227,6x54,5x127 mm.

L'acquisizione dei dati

Scambiare e acquisire i dati in modo efficace tra i singoli sottosistemi e i componenti è di cruciale importanza per la produttività… e il software è il fattore più critico

Francesco Ferrari

In passato i sistemi comunicavano solitamente tramite interfacce programmate singolarmente oppure tramite i device driver. Questo sistema, per quanto efficace, richiedeva però la programmazione delle applicazioni per assicurare l'interoperabilità, una strada che nel tempo non si è dimostrata molto pratica.
Una soluzione interessante per l'industria, soprattutto per quella dell'automazione, in grado di assicurare lo scambio di dati tra le applicazioni di diversi produttori, è arrivata nel 1996 con l'OPC (OLE for Process Control). Con questo tipo di tecnologia i produttori dei terminali utilizzati nell'automazione industriale sono in grado di impostare un server OPC per elaborare i dati dai diversi client OPC come quelli nei controller, sistemi SCADA e dispositivi HMI.
Questo tipo di soluzione è semplice da utilizzare e riduce sensibilmente gli sforzi necessari per implementare le attività di comunicazione fra i device: infatti, è stata impiegata con successo in numerose applicazioni, come per esempio quelle di tipo office per integrare nei sistemi le periferiche, come le stampanti provenienti da diversi produttori.
Lo sviluppo di software per i prodotti compatibili con OPC si appoggia su un'altra tecnologia di Microsoft, quella COM/DCOM (Distributed Component Object Model) con i suoi vantaggi e svantaggi. Per esempio, questa tecnologia ha il vantaggio di una piattaforma caratterizzata da un elevato livello di stabilità grazie alla sua ampia distribuzione.
Per contro, gli sviluppatori si trovano ad affrontare alcune limitazioni come il dispendio di tempo per la configurazione, soprattutto per il fatto che si tratta di una tecnologia strettamente legata al sistema operativo Windows e alle limitazioni nella capacità di controllo dovuta alla natura proprietaria di COM/DCOM.
Un altro esempio è l'Object Linking and Embedding (OLE), un protocollo di scambio dati sviluppato da tempo da Microsoft per le applicazioni di ufficio e che risiede direttamente nel sistema operativo. Questo protocollo permette, per esempio, l'integrazione da fonti esterne di dati in tabelle o anche di integrare tabelle e immagini nei documenti.
In generale, vale la pena di sottolineare che le soluzioni aperte permettono di lavorare servendosi degli strumenti di volta in volta più idonei, consentendo ai sistemi di comunicare senza particolari problemi. Le soluzioni aperte agevolano inoltre il riutilizzo del software esistente, permettendo di liberare tempo prezioso per poter commercializzare più rapidamente i propri prodotti.

Fig. 1 – OPC UA consente di realizzare comunicazioni fra diversi hardware e differenti applicazioni indipendentemente dalla piattaforma e dal sistema operativo utilizzato

L'OPC UA

Per quanto riguarda le interfacce software standardizzate, l'approccio dell'OPC UA(Unified Architecture) è stato

concepito per superare diverse limitazioni di altri sistemi precedenti. Fornisce infatti una completa scalabilità, dal software di controllo integrato ai sistemi di gestione informazioni. Questa tecnologia combina le specifiche precedentemente separate per dati, eventi, oggetti o comandi in un unico standard unificato.
OPC UA dispone di una architettura orientata ai servizi (SOA) con vari livelli di comunicazione e uno stack di comunicazione separata per sostituire la precedente tecnologia COM/DCOM.
Questo protocollo offre funzioni di facile utilizzo per l'accesso ai dati e programmi indipendentemente dalla piattaforma utilizzata: questo si ottiene grazie alla comunicazione diretta tra diverse applicazioni su tutte le piattaforme hardware e i sistemi operativi.
Dato che l'OPC UA utilizza servizi di base e il modello di dati OPC per definire come accedere ai dati, diventa più facile il porting su diverse tecnologie, permettendo lo scambio di dati grezzi e di informazioni pre-elaborate in modo sicuro e affidabile, indipendentemente dal device e dall'ERP.
In pratica, questo protocollo definisce il modo in cui i dati sono scambiati tra i meccanismi convenzionali di trasporto TCP / IP e i modelli di dati definiti dai produttori di dispositivi delle organizzazione di standardizzazione come PLCopen. Una cosa interessante è che questo sistema funziona su reti diverse e, grazie a queste funzioni , i client possono determinare automaticamente quali server sono disponibili e che tipo di dati ciascuno di essi può offrire.
Disponibile in ANSI C, C# e Java, lo stack di comunicazione di OPC UA può essere portato su qualsiasi sistema operativo o hardware embedded e compilato per l'uso con applicazioni multi-thread o single task. Questo consente a qualsiasi dispositivo intelligente di agire come server, indipendentemente dal produttore, dal linguaggio di programmazione e dal sistema operativo, eliminando la necessità di un PC per le intermediazioni.

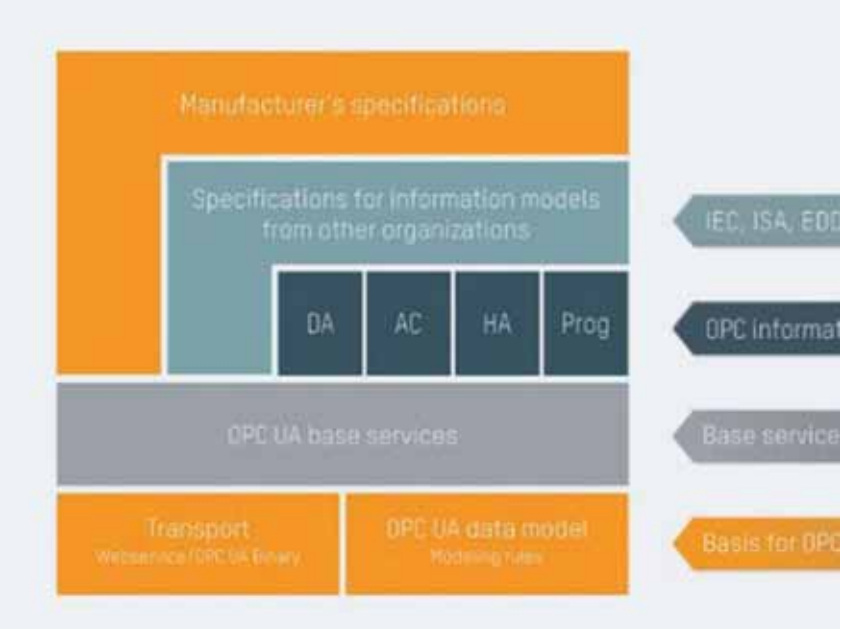


Fig. 2 – OPC UA utilizza i servizi di base a le informazioni del modello OPC per definire le modalità di accesso ai dati

Un esempio

Automation Studio 4 di B&R consente la progettazione dei PLC in tutti i linguaggi IEC 61131-3, in CFC e in C, ma anche la progettazione object-oriented in C++. Oltre a consentire ai programmatori di lavorare nel linguaggio preferito, questo permette anche di integrare il codice esistente in modo semplice e veloce.
La disponibilità di blocchi funzione PLCopen, come quelli per il controllo di movimento e la sicurezza, semplifica ulteriormente la programmazione; lo stesso vale per l'integrazione dei codici generati in modo automatico dagli strumenti di simulazione.
La condivisione dei file dei progetti avviene esclusivamente in formato XML, che garantisce una comunicazione aperta con i sistemi di terzi come i software di gestione dei materiali e di pianificazione della produzione. Un ulteriore supporto viene fornito dall'accesso diretto ai database tramite l'interfaccia SQL.
Questo sistema permette di avere uno scambio dati bidirezionale con sistemi CAD e i relativi vantaggi. La generazione automatica del codice, a partire da modelli di simulazione, contribuisce infatti ad allineare il software con la progettazione meccanica già in una fase molto precoce del processo di sviluppo. L'impegno di programmazione si riduce ulteriormente grazie alla possibilità di creare singoli componenti o interi moduli tramite software CAD avanzati utilizzando i dati generati dalle simulazioni della cinematica e della dinamica dei sistemi.
Automation Studio consente agli sviluppatori di programmare, provare e ottimizzare algoritmi e anelli di controllo aperti e chiusi, sequenze di movimenti e interfacce di visualizzazione, in un unico ambiente di sviluppo. In sostanza, grazie all'impiego di architetture software e di comunicazione aperte questa piattaforma di sviluppo integrata e dotata di sistema operativo real-time supporta dall'inizio alla fine lo sviluppo in tempi brevi di soluzioni complete.

Problematiche per la messa a punto di Small Form Factor rugged con parti commerciali

È sempre più difficile scegliere l'ottimo fra prestazioni, riutilizzabilità e costi nei sistemi embedded quando si cerca di implementare insieme sottosistemi commerciali e rugged

Lucio Pellizzari

Le schede SFF, Small Form Factor, per applicazioni embedded continuano a essere troppo custom per poter semplificare lo sviluppo dei sistemi e d'altra parte non si può evitare che i costruttori proteggano la proprietà intellettuale che preserva il valore di mercato dei loro prodotti. Ciononostante, sono sempre più numerose le schede destinate alle applicazioni industriali, militari e aerospaziali che ospitano parti essenzialmente commerciali sia nelle caratteristiche tecniche sia nel costo. Per chi progetta questi sistemi ibridi si tratta di cercare di soddisfare tutti i requisiti rugged e mission-critical, tipici delle applicazioni impegnative, ma nel contempo assicurarsi di utilizzare componenti e sottosistemi che, oltre a essere più economici nel costo iniziale, siano anche più rapidamente aggiornabili quando c'è bisogno di stare al passo con il rapido evolvere delle tecnologie elettroniche e telecom.

I piccoli formati, o Small Form Factor, hanno caratteristiche e dimensioni che è sempre difficile far convivere in soluzioni ibride capaci di ospitare insieme schede COM Express, miniPCIe, PC/104, Qseven o di altro tipo senza il supporto di una buona scheda madre con sopra tutti gli zoccoli che servono. Questo problema si complica se si pensa di affiancare gli zoccoli per le schede commerciali agli zoccoli per le schede rugged e i connettori per le interfacce con caratteristiche commerciali ai connettori rugged. È ovvio che le prestazioni, e soprattutto la robustezza, sono molto diverse nei rugged, che oltretutto sono spesso realizzati esclusivamente con progetti custom, fatti apposta per talune specifiche applicazioni. Per contro, i rugged costano di più e perciò sono anche fabbricati per durare di più, il che significa che non si può pensare di sostituirli a metà del tempo loro previsto perché vorrebbe dire pagarli il doppio. Ci sono però applicazioni nelle quali solo alcune parti del sistema devono essere necessariamente rugged, mentre alcune altre non hanno requisiti particolarmente severi e si possono scegliere con caratteristiche commerciali senza rischi.

In genere si distingue fra le interfacce board-to-board e bo-

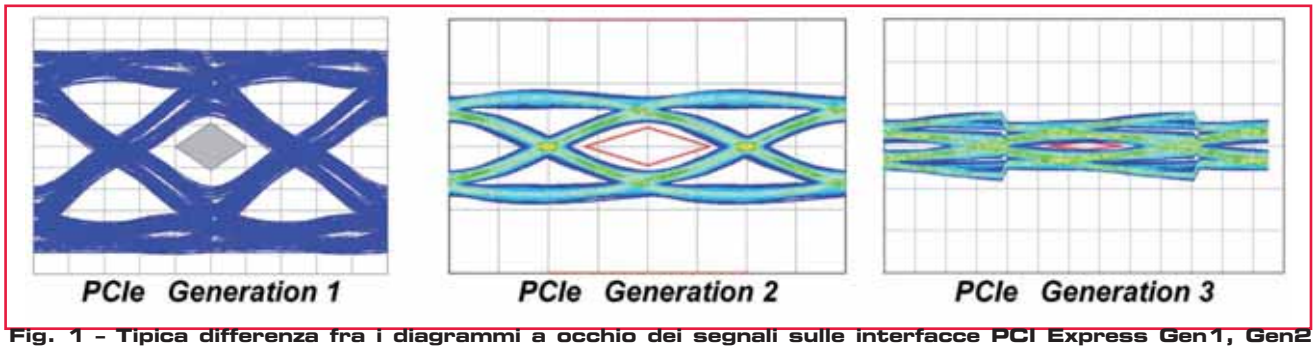


Fig. 1 - Tipica differenza fra i diagrammi a occhio dei segnali sulle interfacce PCI Express Gen1, Gen2 e Gen3

ard-to-I/O perché hanno diverse funzionalità. Le prime sono essenzialmente dei backplane con caratteristiche custom tali da poter ospitare slot multipli per allacciare diversi tipi di schede, ma comportano il rischio di limitare la riutilizzabilità dei sistemi. Le seconde coinvolgono tipicamente una gran quantità di cablaggi che non sempre si può ridurre usando dei mezzanini impilati uno sopra l'altro. In entrambi i casi si rischia di aumentare il volume di connettori e cablaggi, accrescendone l'ingombro oltre quello delle schede stesse, e d'altra parte non si può nemmeno pensare di salvarsi utilizzando cavi e connettori multifunzione perché vorrebbe dire renderne più complessa la gestione e perciò meno affidabile, oltre che ulteriormente più costosa nel caso delle schede rugged.
In effetti, queste ultime possono avere requisiti molto diversi se destinate a una centrale per telecomunicazioni piuttosto che alla locomotrice di un treno oppure a bordo di un jet militare e qui ricorre l'eterno dilemma della progettazione elettronica perché, come sempre, quanto più si specializza il progetto di un sistema embedded e tanto più se ne limitano le possibilità applicative mentre, viceversa, se si progetta un sistema in modo tale da supportare un'ampia varietà di interfacce e periferiche, lo si rende inevitabilmente meno efficace a svolgere funzionalità specifiche. È il progettista che può decidere quante e quali parti devono essere rugged e custom e quante e quali possono essere di tipo commerciale, valutando i requisiti che gli vengono richiesti in termini di dimensioni delle schede, quantità dei cablaggi, previsioni di costo, riutilizzabilità dei sottosistemi, manutenzione e aggiornabilità a livello di sistema.

Integrità dei segnali ad alta velocità

Le nuove interfacce ad alta velocità come PCI Express 3.0 a 8 GTps (Giga Transfers per second), USB 3.0 a 5 Gbps e SATA a 6 Gbps, e la recente diffusione dei display ad alta definizione stanno rendendo sempre più critico il progetto delle schede con piccolo fattore di forma SFF. Per garantire l'integrità dei segnali sugli I/O ad alta velocità occorre progettarne accuratamente le caratteristiche di impedenza, anche quando si sceglie di accorpare due o più schede attraverso i formati standard più comuni come COM Express e PC/104.
Intel definisce l'integrità dei segnali come la verifica che tutti i segnali siano trasferiti correttamente senza interferenze o accoppiamenti fra le forme d'onda capaci di degradarne la riconoscibilità o generare inquinamento elettromagnetico, che può danneggiare il sistema che li ospita o i sistemi vicini. In ciò sono coinvolte tutte le componenti della linea di trasmissione da chip a chip e quindi, oltre alle interfacce, anche i connettori e i cavi verso i display come DisplayPort, DVI o HDMI, oggi drasticamente più complessi dei predecessori Lvds e VGA. Oltre a essere più veloci, questi collegamenti sono anche a basso voltaggio e perciò la minor ampiezza degli impulsi limita la tolleranza sul riconoscimento dei simboli soprattutto nei convertitori A/D dove il rumore può deteriorare le forma d'onda specialmente al momento delle transizioni di livello che ad alta frequenza sono piuttosto ripide. Per migliorare l'integrità dei segnali e rendere più efficaci e affidabili i sottosistemi di riconoscimento dei simboli occorre aumentarne la complessità e se si tratta di sistemi rugged anche il costo. Di nuovo, si deve scegliere se progettare sistemi più specifici e più efficienti ma meno riutilizzabili oppure più generici ed economici ma con prestazioni inferiori.
L'impedenza intrinseca del tratto percorso dai segnali ha un ruolo fondamentale, perché dipende dal dimensionamento delle linee di trasmissione, delle

piste sulla scheda stampata e di tutti i connettori ma nelle condizioni ideali dovrebbe essere sempre uguale anche nei punti di contatto fra le parti perché altrimenti si creano delle riflessioni che fanno perdere energia ai segnali degradandone la riconoscibilità. Purtroppo, in realtà non è così perché l'accoppiamento fra le schede, i connettori e i cavi non è mai perfetto e peggiora in proporzione con la velocità dei segnali e con la vicinanza fra le linee, imponendo restrizioni più severe proprio alle interfacce di nuova generazione. Un po' si migliora con le linee differenziali che riescono ad abbattere le interferenze comuni, perché i simboli sono riconosciuti come differenza fra due linee annullando gli offset dovuti al rumore indipendentemente dalla velocità dei segnali. Tuttavia, lo svantaggio delle linee differenziali è il basso voltaggio del segnale differenziale che può far diminuire l'energia dei segnali nelle tratte più lunghe e soprattutto ad alta velocità può deteriorare il riconoscimento dei simboli nei collegamenti oltre qualche dm.
Una tecnica molto diffusa per la verifica del corretto setup delle connessioni è l'In-Circuit-Testing, che si esegue facendo passare un segnale noto attraverso un'interfaccia e misurando ciò che passa e ciò che viene riflesso o in qualunque modo alterato. Purtroppo con i moderni package BGA da centinaia di sfere di contatto questa metodologia è improba e pertanto oggi bisogna ricorrere a strumenti fatti apposta per l'In-Signal-Testing e affiancare anche degli adeguati strumenti di simulazione pre-layout e post-layout per valutare le prestazioni dei connettori, dei cablaggi e delle saldature dei circuiti integrati sulle schede. La messa a punto delle interfacce può essere considerata una fase preliminare nel ciclo di sviluppo di un sistema embedded e, tuttavia, incide pesantemente sull'integrità dei segnali, sulla qualità delle prestazioni e perciò anche sulle decisioni del progettista al momento della scelta fra componenti e sottosistemi rugged oppure commerciali.

Test analogici su simboli digitali

D'altro canto, la scarsa integrità dei segnali non è sempre rilevabile con i test preliminari sui sistemi, perché non si è mai sicuri di prevedere davvero tutto ciò che può succedere nell'ambiente applicativo che li circonda nel corso del loro intero ciclo vitale. I segnali nei sistemi e nei sottosistemi limitrofi possono sommarsi in alcuni momenti assolutamente casuali, nei quali si trovano tutti al loro massimo picco e pertanto diventano per brevi momenti aggressivi generando rumore intermittente, che a sua volta danneggia alcune brevi sequenze di simboli. Questi eventi possono sfuggire ai test preliminari sulle interfacce proprio perché sono temporanei e perciò richiedono degli approfonditi metodi di verifica Test-to-Fail capaci di individuare i peggiori scenari possibili (Worst-Case Scenario). Nelle moderne interfacce PCIe

Fig. 2 – Un adattatore Connect Tech che consente di installare le schede PCIe/104 e PCI/104-Express negli slot standard PCI Express

Gen3, Sata 6 Gbps e USB 3.0 questa problematica è stata considerata e oggi alla loro accensione parte immediatamente l'inizializzazione di entrambi i transceiver di trasmissione e di ricezione, con annessa prova di trasferimento sulla linea finalizzata a negoziare la velocità di trasmissione più adeguata per minimizzare rumore, errori e malfunzionamenti e migliorare quanto più possibile l'integrità dei segnali.
Si noti che, soprattutto con i segnali ad alta velocità, gran parte del lavoro occorrente per affinare e rendere maggiormente immuni da errori le forme d'onda dei simboli binari si fa considerando gli impulsi di tensione che li trasportano dal punto di vista analogico. Purtroppo, per questo motivo gli strumenti per catturare, analizzare e verificare i segnali alle bande di frequenza dell'ordine della decina di GHz sono costosi e, inoltre, i test devono anche essere affiancati da un'adeguata fase di simulazione preliminare. Per di più, questi costi crescono proprio quando si cerca di far convivere nello stesso sistema i sottosistemi di diversi costruttori e si scopre che nei punti di contatto non c'è mai un accoppiamento adeguato. A maggior ragione, quando si affiancano sottosistemi rugged e commerciali, i disaccoppiamenti a livello delle interfacce possono richiedere un lungo lavoro di messa a punto per ottimizzare l'integrità dei segnali, con la conseguenza di aumentare inevitabilmente la probabilità di errore nel funzionamento a regime del sistema. Questo è un rischio da valutare attentamente prima di mescolare insieme i componenti commerciali e rugged.

L'impatto sull'affidabilità dei sistemi della gestione remota basata su cloud

Un accesso semplice e centralizzato ai dati di un sistema permette di ridurre sensibilmente i costi di gestione e di manutenzione in qualsiasi tipo di applicazioni embedded

Dirk Finstel
Executive vice president
Global Module Computer Product Segment
ADLINK

È fuor di dubbio che i sistemi embedded "fanno girare" il mondo. Qualunque sia il campo applicativo – trasporti, difesa, infotainment, medicale, telecomunicazioni o industriale – è necessario ottimizzare le prestazioni offerte dalla tecnologia perché questi sistemi possano assolvere il loro compito nel miglior modo possibile. I sistemi devono essere stabili e affidabili per far girare applicazioni critiche, che spesso richiedono continuità di funzionamento e bassi consumi e si trovano a operare in ambienti dove sono presenti forti escursioni termiche, sollecitazioni e vibrazioni. Interruzioni e periodi di inattività non sono ammissibili e ciò rappresenta un requisito di prestazione di fondamentale importanza per i sistemi connessi. Garantire il necessario livello di stabilità tecnologica è una sfida progettuale non indifferente e richiede un costante miglioramento dei tool per il controllo e la gestione del sistema, che devono essere in grado di rilevare potenziali problemi prima che questi si manifestino. La connettività sempre più pervasiva ha un notevole impatto sulle modalità utilizzate dagli sviluppatori di sistemi per affrontare questa sfida. La sempre più ampia diffusione dell'Internet of Things (IoT), dove dispositivi „intelligenti" condividono dati in tempo reale, ha avuto come conseguenza una progressiva evoluzione dei sistemi embedded, che si sono trasformati da sistemi isolati a piattaforme „intelligenti" e connesse.

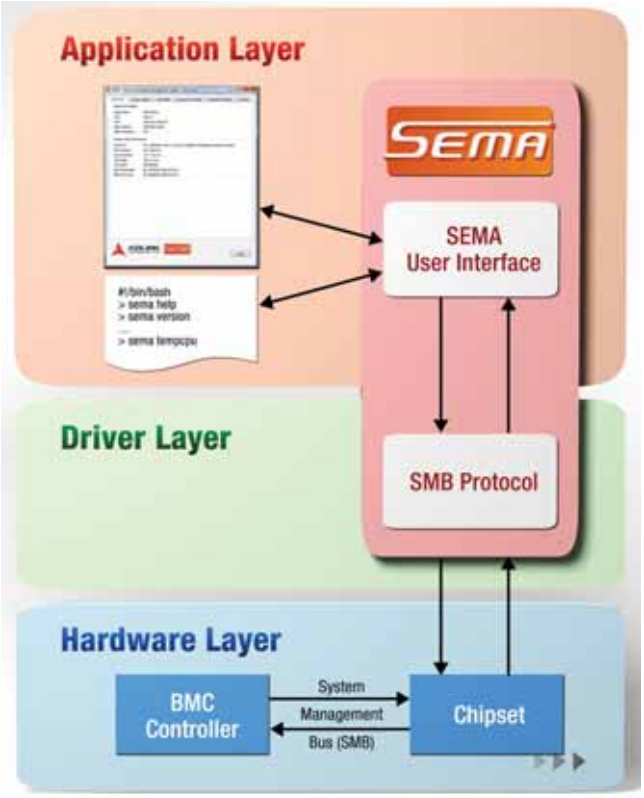


Fig. 1 – SEMA (Smart Embedded Management Agent) di ADLINK è un insieme di funzioni embedded integrate che consente il monitoraggio e la gestione remota basate su cloud. Gli operatori di sistema possono controllare diversi parametri hardware per aumentare sia la durata dei sistemi embedded sia l'affidabilità grazie alla manutenzione preventiva

Ciò comporta vantaggi non indifferenti nella gestione e manutenzione dei sistemi che non erano disponibili nel caso di sistemi non connessi; gli operatori di sistema sono ora in grado di sfruttare l'accesso al cloud per implementare una gestione centralizzata e proattiva che permette di ridurre i costi grazie alla manutenzione preventiva e alla possibilità di evitare riparazioni in loco. Ad esempio, invece di reagire a un errore di sistema una volta che questo si è verificato, gli operatori possono ora collegarsi in remoto per visualizzare lo stato attuale del sistema, incidere sulle prestazioni e persino prevedere, prevenire o risolverere malfunzionamenti critici del sistema. Ancora più importante, un accesso di questo tipo e il valore aggiunto che ciò comporta può essere utilizzato non solo da quelle realtà industriali che hanno un'intrinseca necessità di monitorare reti distribuite, bensì essere implementato nella quasi totalità delle applicazioni embedded.

Ridurre i costi mediante decisioni appropriate

La conoscenza delle condizioni di un sistema è essenziale per garantirne la stabilità. Grazie alla disponibilità di una gran quantità di dati, gli operatori possono inviare il personale di assistenza prima che si verifichi un guasto del sistema oppure gestire il sistema stesso in modo da evitare una costosa e inutile chiamata al servizio di assistenza. L'eliminazione di interventi in loco da parte dei tecnici rappresenta un notevole vantaggio per gli operatori che devono gestire reti distribuite – contribuendo a incrementare i profitti e la loro quota di mercato grazie alla riduzione dei costi di manutenzione e all'aumento della qualità del servizio. Al giorno d'oggi middleware „intelligenti" – essenzialmente uno strato di software che permette di effettuare operazioni di analisi e gestione remote attraverso una semplice interfaccia grafica (GUI) – contribuiscono a semplificare l'acquisizione delle informazioni relative alle condizioni del sistema in tempo reale. Gli operatori sono ora in grado di identificare e risolvere rapidamente problemi, quali ad esempio incrementi di temperature oppure variazioni dei consumi di potenza o della velocità delle ventole.
A causa ad esempio del malfunzionamento di una ventola, il processore può surriscaldarsi e danneggiarsi. Il sistema potrebbe non funzionare più correttamente e le operazioni di riparazione potrebbero essere rallentate a causa della necessità di sostituire componenti specifici.
Nel caso in cui questi componenti non fossero disponibili, i sistemi critici potrebbero guastarsi e provocare costosi fermi macchina che possono durare da poche ore ad alcuni giorni.
Nel caso si utilizzi la gestione remota, gli operatori sono in grado di garantire l'invio del personale addetto alle riparazioni laddove è presente un sistema che evidenzia potenziali criticità, prima quindi che possa verificarsi un guasto.

Fig. 2 – Utilizzando il dashboard dell'agente remoto è possibile impostare limiti per diversi tipi di dati del sistema. Nel momento in cui vengono superate le soglie definite, l'operatore è immediatamente informato via e-mail o attraverso una notifica scritta

Nel frattempo i sistemi possono essere riconfigurati da remoto per assicurarne l'operatività. Gli operatori possono trarre un vantaggio ancora maggiore dalla gestione remota con l'analisi dei dati del sistema. Essa fornisce i trend delle prestazioni sul lungo periodo e permette di prevedere e prevenire guasti del sistema prima di qualsiasi segnale di allarme, mentre dà la possibilità di incrementare la durata operativa del sistema mediante il monitoraggio e il controllo di vari parametri hardware.

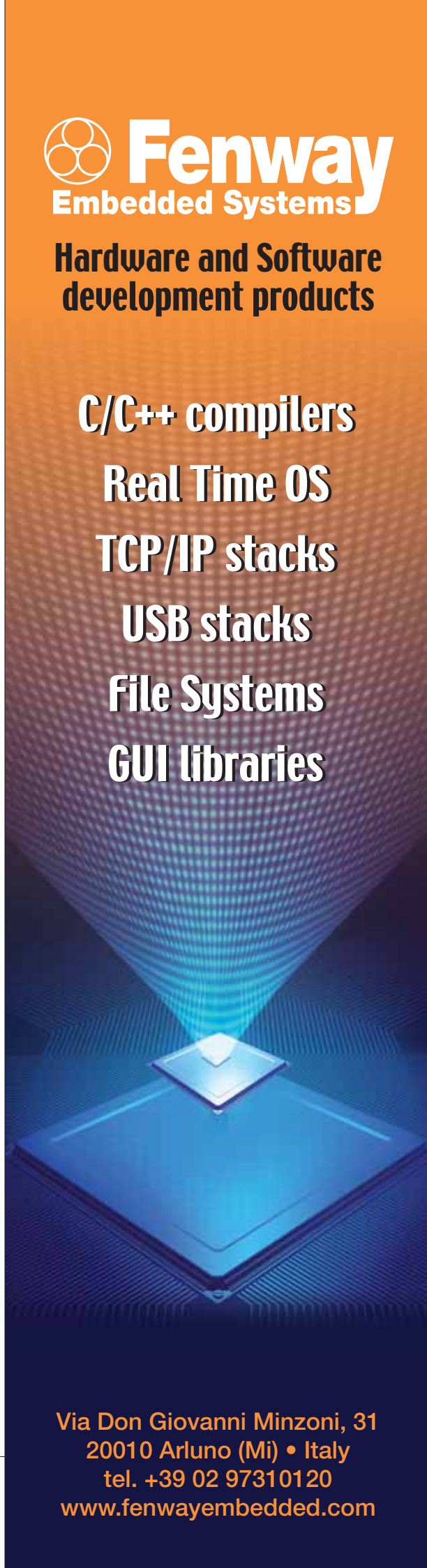
Integrazione della gestione remota nelle soluzioni embedded

Anche se la connessione con i dispositivi remoti può essere effettuata in diversi modi, sono in ogni caso richiesti componenti hardware, firmware e software. ADLINK utilizza un controllore BMC (Board Management Controller): inizialmente progettato per svolgere compiti di sequenzializzazione della potenza, questo BMC è evoluto nel corso del tempo integrando un numero sempre maggiore di funzionalità utili per il controllo e la gestione della scheda. La misura della corrente di alimentazione per ottenere un'"istantanea" del consumo di potenza del sistema è solo un esempio di queste nuove funzionalità.
La compatibilità con le più recenti specifiche EAPI (Embedded Application Programming Interface) semplifica il porting delle chiamate esistenti sul controllore BMC.
Una delle più importanti funzioni del sistema per la gestione remota è fornire l'interfaccia tra l'hardware e il sistema operativo. Il controllore BMC in primo luogo acquisisce tutte le informazioni necessarie dal chipset e da altre fonti. Utiliz-

zando il bus per la gestione del sistema (SMB – System Management Bus), il livello applicativo carica i dati e li presenta all'utente, visualizzandoli nel menu del BIOS o su una dashboard (in pratica un pannello di controllo) di semplice e immediata comprensione adatta per la supervisione e la ricerca dei guasti (troubleshooting). Gli operatori di sistema possono visualizzare e prendere in considerazione i grafici che illustrano le statistiche "vitali" del sistema come il consumo di potenza o le temperatura sia della CPU sia della scheda, che vengono richiesti ogni secondo e scritti (opzionalmente) in un file di log di sistema (che tiene la registrazione delle attività compiute) memorizzato in locale e utilizzabile dall'amministratore del sistema.
I dati sono scritti come testo ASCII in chiaro in colonne delimitate da tabulazioni in modo da semplificare l'importazione in qualsiasi tipo di spreadsheet, programma o tool per l'elaborazione dei dati. Gli utenti possono inoltre accedere a informazioni di natura generale relative alla scheda, ad aree di memoria e accesso sicuro, oltre che a controlli delle ventole, GPIO e bus I2C. Il controllore BMC utilizza una tecnologia "intelligente" per il controllo della ventola e mette in correlazione automaticamente la temperatura misurata della CPU alla velocità del ventola.
Attraverso i loro controllori della scheda embedded, gli agenti (in pratica programmi che raccolgono informazioni) per la gestione remota locali forniscono una quantità definita di memoria per i dati dell'utente finale. Questa area di memoria è ottimizzata per immagazzinare numeri seriali, chiavi, dati di configurazione e altre informazioni sensibili o specifiche della scheda, poiché essa resta indipendente dal BIOS e non viene cancellata o ripristinata durante gli aggiornamenti del BIOS.
Un'area sicura separata mette a disposizione uno spazio di memoria aggiuntiva, ideale per immagazzinare dati critici come ad esempio i codici delle chiavi di sicurezza. Questa area può essere protetta mediante un fusibile hardware programmabile una sola volta (OTP) per garantire il massimo livello di sicurezza e fornisce funzionalità simili a quelle dei moduli TPM (Trusted Platform Module) o delle schede SIM. Gli operatori di sistema possono assegnare un'unica chiave al loro sistema, in modo da impedire operazioni di lettura o copiatura senza il permesso dell'amministratore.
Le informazioni disponibili dopo il verificarsi di un guasto del sistema o di un modulo comprendono temperature minime e massime della CPU e del sistema, oltre alla causa che ha provocato l'ultimo riavvio del sistema: esse possono risultare utili per l'analisi del guasto del modulo o del sistema.

Il valore aggiunto delle strategie "Device-to-Cloud"

La possibilità di includere, nell'ambito delle tecnologie di gestione remota, l'accesso sicuro al cloud, risulta particolarmente efficace per gli amministratori di sistema.
La gestione remota basata su cloud assicura la disponibilità su base continua dei dati del sistema, che possono essere utilizzati per aumentare l'uptime (ovvero la sua disponibilità) del sistema grazie alla possibilità di prevedere e reagire a eventuali anomalie o guasti del sistema senza incorrere nei costi (e nei tempi) associati alla manutenzione in loco di uno o più dispositivi distribuiti. Al crescere della diffusione della tecnologia IoT corrisponde un aumento della competitività, ragion per cui i fornitori richiedono la disponibilità di sistemi realmente "intelligenti" che assicurino la massima flessi-



bilità e permettano di avere una conoscenza dettagliata del comportamento del sistema in relazione a una pluralità di ambienti e carichi di elaborazione. Una conoscenza di questo tipo garantisce un vantaggio competitivo, una riduzione dei costi, un aumento dell'uptime del sistema e favorisce un'installazione e messa in esercizio (deployment) più efficiente in un gran numero di applicazioni nuove e innovative. La connettività cloud ha favorito l'evoluzione del grado di "intelligenza" del middleware rispetto alla tecnologia di gestione remota delle precedent generazioni.
Adottando un'architettura cloud server e uno stack M2M (machine-to-machine) che risiede al di sopra del midlleware "intelligente", i dispositivi embedded possono collegarsi al cloud senza requisiti di progetti addizionali. Il trasferimento dei dati verso il cloud in modalità push (ovvero automatico) consente agli operatori di verificare, monitorare e gestire le prestazioni di un sistema da un'unica locazione centrale, con conseguente aumento dell'affidabilità e riduzione dei costi di gestione.
Ad esempio, lo stack M2M della soluzione SEMA (Smart Embedded Management Agent) Cloud di ADLINK trasferisce i dati del sistema in modalità push al server cloud attraverso un qualsiasi collegamento TCP/IP – 3G, LAN o LAN wireless (Fig. 1). I manager del sistema hanno accesso in maniera molto semplice ai dati e alle analisi degli stessi utilizzando dispositivi quali desktop PC, tablet o smartphone.

Gestione "intelligente" del sistema

Utilizzando la connettività cloud, vi sono tre differenti scenari che coprono le principali necessità degli operatori di sistemi. Questi scenari possono essere classificati come segue: informazione, analisi e creazione di eventi, gestione multipla di dispositivi.

Informazione – Nel momento in cui i sistemi sono disponibili, gli operatori possono rilevare le loro prestazioni. La gestione remota basata su cloud favorisce questo processo consentendo di effettuare rilevazioni in ogni momento e in qualsiasi luogo. In un contesto di questo tipo, l'agente di gestione embedded carica su base continuativa i dati attraverso un collegamento cifrato che usa il protocollo TLS (Transport Layer Security – il successore di SSL), che sono visualizzati sul dashboard (Fig. 2). Su questo pannello informativo sono riportate anche informazioni relative alla temperatura e ai consumi di potenza di differenti parti di un sistema embedded. Poiché è possibile accedere ai dati in qualsiasi momento, gli operatori sono in grado di determinare se le prestazioni sono accettabili anche nel caso in cui determinati valori variano rispetto alle impostazioni prefissa
Analisi dei dati e creazione degli eventi – Il medesimo dashboard consente agli operatori di sistema di definire i

Fig. 3 – Gli operatori possono controllare in modo remoto diversi parametri di un sistema, come ad esempio la velocità di una ventola; eventuali azioni sono innescate in modo automatico sulla base delle prestazioni e dello "stato di salute" del sistema, in modo da prevenire danni al sistema in caso di malfunzionamento

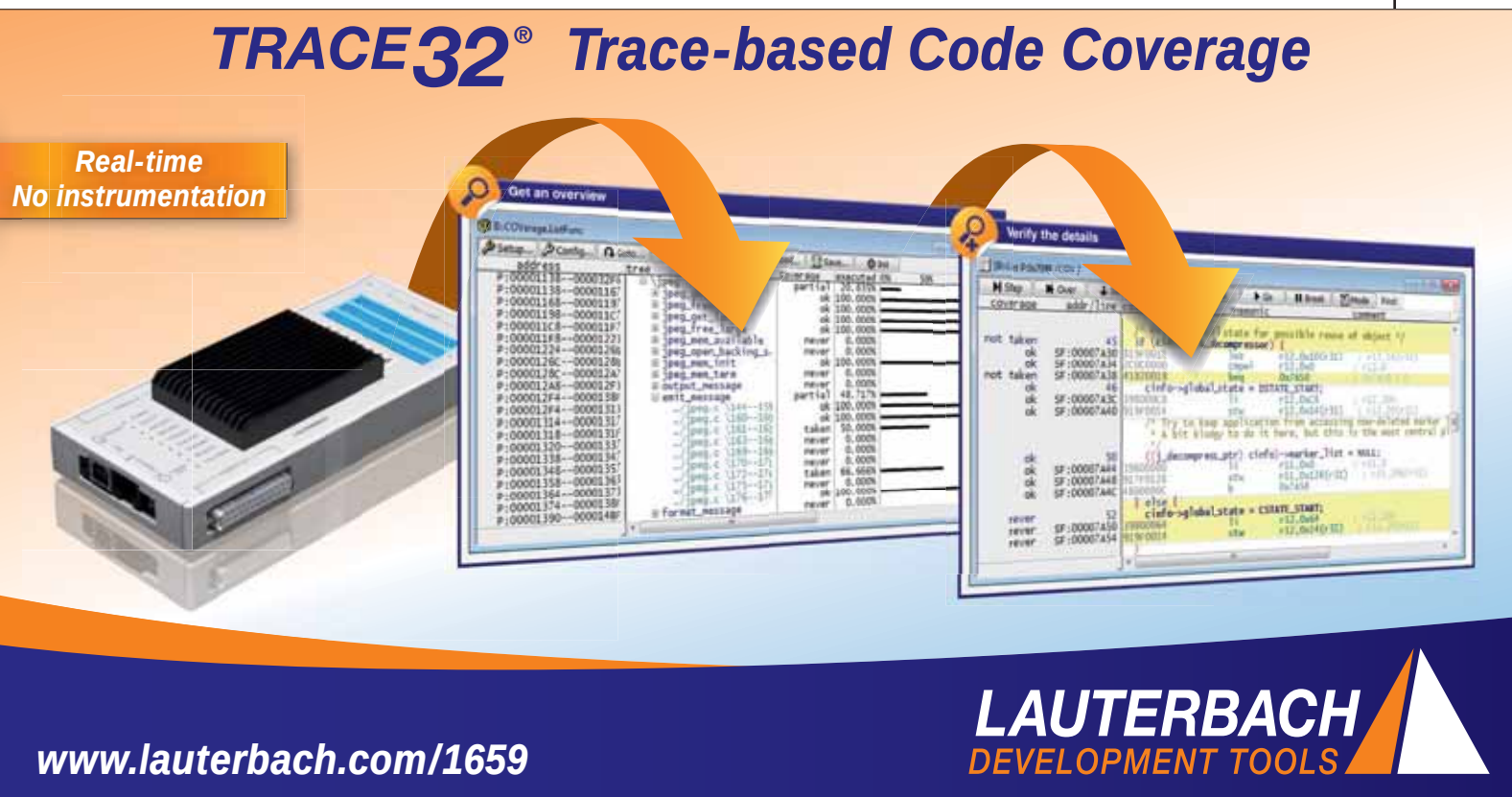
limiti di parecchie tipologie di dati. In questo caso il software applicativo analizza continuamente i dati in entrata e nel caso vengano raggiunti i limiti definiti dall'utente, un allarme darà origine a un evento. Si consideri ad esempio un dispositivo mobile dotato di due pacchi di batterie: la batteria primaria fa funzionare il dispositivo mentre la batteria secondaria è impiegata come backup. Quest'ultima entra in funzione nel momento in cui la capacità di potenza scende al di sotto del 10%; questa informazione è riportata dall'agente di gestione embedded che si occupa del monitoraggio del consumo di potenza. Se la capacità della batteria primaria scende al di sotto del 10%, viene generato un allarme e l'agente remoto commuta istantaneamente sul pacco di batterie secondario. Contemporaneamente l'operatore del sistema è informato – via SMS o tramite e-mail – che il dispositivo deve essere caricato.
Gli operatori possono interagire in modo pro-attivo – e non solo semplicemente reagire – con il sistema per garantire una maggiore affidabilità, affrontando in anticipo potenziali

problemi e reagendo in modo molto più rapido in presenza di malfunzionamenti del sistema. Si consideri ad esempio un distributore di ghiaccio ubicato in una stazione di servizio.
L'apparecchio, del valore di qualche migliaio di dollari, è presente nella stazione ma appartiene a un costruttore esterno. Problemi di temperatura possono generare danni di notevole entità. L'implementazione di dispositivi di monitoraggio M2M in grado di avvertire immediatamente i responsabili dell'insorgere di qualche problema, contribuisce in modo efficace a prevenire eventuali danni e relative perdite finanziarie e di immagine.

Gestione di più dispositivi – Un ulteriore vantaggio degli agenti embedded che supportano la tecnologia cloud è la possibilità di controllare in modo remoto i parametri di sistema: specifiche configurazioni impostate dall'utente innescheranno l'esecuzione automatica di determinate azioni. Ciò può essere replicato per un gran numero di dispositivi, consentendo la gestione di un parco (di apparati) o di più dispositivi (Fig. 3).
Sfruttando lo stack M2M, gli utenti possono predisporre in maniera molto semplice un'applicazione cloud per controllare più dispositivi, che si preoccupa di esaminare lo "stato di salute" attuale dei sistemi embedded connessi. Prima che un dispositivo si guasti, l'applicazione può individuare il malfunzionamento attraverso queste funzioni di gestione remota, consentendo quindi una reazione rapida, come ad esempio la sospensione dell'attività del sistema prima che possa subire qualche danno. Gli operatori possono ripristinare il sistema, nonché verificare e correggere eventuali malfunzionamenti. Ciò permette di ridurre i costi di riparazione nonché di ridistribuire i carichi di lavoro da un sistema all'altro, eliminando i tempi di fermo macchina nel caso di guasto di un'apparecchiatura.
Quando gli amministratori sono in grado di reagire prima del verificarsi di guasti hardware di una certa entità, aumenta la durata del sistema. Un semplice incremento della temperatura della CPU permette di illustrare questo concetto ed evidenziare come agisce la gestione remota di un dispositivo. Il controllore BMC trasferisce i dati all'agente, che reagisce immediatamente cercando di aumentare la velocità della ventola. Se questa operazione non ha successo a causa di un guasto hardware, l'attività del sistema viene sospesa da remoto per ragioni di sicurezza, mentre all'operatore viene inviata immediatamente una notifica. Una volta ricevuto l'avviso, il manager del sistema può sostituire la ventola e assicurare un riavvio del sistema in tempi brevi.

Un futuro promettente per i servizi M2M

Un approccio centralizzato basato su cloud ben si presta all'implementazione di un modello "intelligente" per i servizi di assistenza, dove gli operatori di sistema possono attivare una sottoscrizione in base al livello di monitoraggio e gestione più idoneo per le loro applicazioni e numero di dispositivi (Fig. 4).
Al crescere della diffusione delle strategie M2M – in settori quali sanità, smart metering, case "intelligenti", POS e attività bancarie al dettaglio, sistemi di fabbrica ed edifici connessi – le prospettive per il settore dei servizi "intelligenti" si fanno sempre più promettenti. Secondo i dati di una recente analisi condotta da Juniper Research, il fattu-



rato globale dei servizi M2M raggiungerà quota 20 miliardi di dollari nel 2015, alimentato da produttori e sviluppatori che vogliono semplificare il processo di introduzione e implementazione di strategie M2M sicure per l'utente finale.
La transazione e l'accesso a dati sensibili mediante applicazioni M2M basate su cloud richiede un'attenta valutazione della sicurezza a livello sia di dispositivo, durante la trasmissione dati, sia dell'ambiente cloud. A livello di dispositivo è possibile utilizzare tool di controllo basati sul software (come ad esempio whitelist) per proteggere dati elaborati e memorizzati localmente.
Come visto in precedenza, protocolli cifrati sono impiegati per il collegamento tra dispositivi distribuiti e i loro punti di accesso ai dati basati su cloud. All'interno del cloud, le aziende che si occupano di hosting dispongono di un vero e proprio arsenale di tool software e metodologie di cifratura per la protezione dei dati residenti su server virtualizzati.
Alcune applicazioni embedded di tipo tradizionale sono intrinsicamente "predisposte" per i servizi di gestione remota.
Applicazioni quali gestione di flotte, pubblica sicurezza, monitoraggio di sottostazioni che erogano servizi di pubblica utilità o, più in generale, qualsiasi implementazione che preveda servizi sul campo o la presenza di reti distribuite su larga scala, sono già pronte a supportare i progressi che sono stati fatti nel campo della gestione e dell'accesso remoti. Tuttavia i servizi di gestione basati sul Web hanno un campo applicativo molto più vasto, aprendo nuove opportunità per l'intera gamma di applicazioni embedded. Realtà per le quali la gestione remota non era un requisito ma avrebbe potuto rappresentare un'opportunità, ora possono accedere in modo semplice a dati sofisticati e ottenere un vantaggio competitivo tangibile.
I sistemi si possono collegare utilizzando la tecnologia wireless 3G, ma possono anche semplicemente trovarsi all'interno di una centrale dove ricevono i dati attraverso connessioni Internet wireless o cablate dai vari apparati presenti nello stabilimento. Per effettuare l'accesso al cloud è sufficiente anche una sola unità, così da permettere ai produttori di tutti i tipi di beni commerciali di attingere in tempo reale ai dati del sistema.
Apparati medicali, sistemi di automazione industriale, apparecchiature di ufficio oppure dispositivi fissi o che vengono trasportati sul campo – in pratica ogni applicazione che integra una scheda embedded – rappresenta una candidata ideale per l'utilizzo dei servizi di monitoraggio remoto basati su cloud. Questi tool e servizi possono anche prevedere la possibilità di effettuare aggiornamenti remoti del software e del sistema operativo consentendo agli utenti di aggiornare con facilità il firmware e potenziare le prestazioni del BIOS in modalità wireless, aggiungendo caratteristiche avanzate e trasferendole ai dispositivi presenti sul campo.

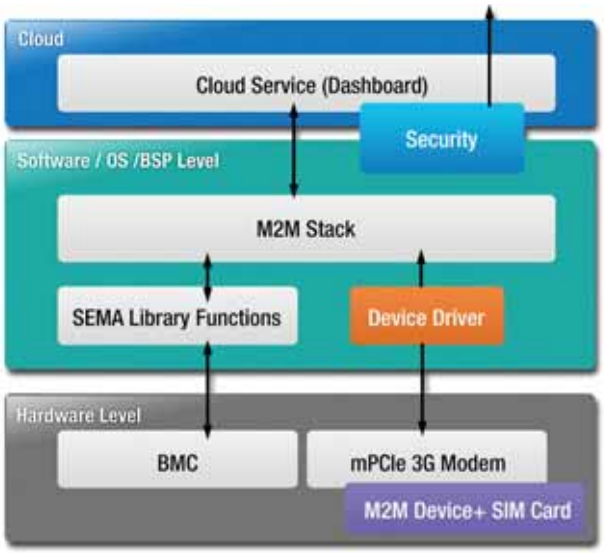


Fig. 4 – Applicazioni quali gestione di flotte, pubblica sicurezza, monitoraggio di sottostazioni che erogano servizi di pubblica utilità o, più in generale, qualsiasi implementazione che preveda servizi sul campo o la presenza di reti distribuite su larga scala, sono già pronte a supportare i progressi che sono stati fatti nel campo della gestione e dell'accesso remoti

I sistemi embedded connessi possono generare e raccogliere una grande quantità di dati sulle prestazioni del sistema – e i progettisti stanno ora sfruttando la tecnologia cloud per condividere questi dati al fine di ridurre i costi e migliorare l'affidabilità.
La gestione remota elimina la necessità di avere un'assistenza locale per effettuare la manutenzione e la ricerca guasti di dispositivi distribuiti: ciò permette di ridurre i costi associati ai trasferimenti del personale e al fermo macchina.
Grazie all'accesso al cloud si possono osservare i sistemi critici da una locazione centralizzata: gli operatori possono rimanere informati sullo stato e sulle condizioni del sistema e sfruttare in tempo reale le doti di "intelligenza" del sistema per prendere decisioni migliori e più informate riguardo al servizio e alle prestazioni.
Il servizio ha una valenza più strategica perché gli amministratori influenzano e interagiscono con le prestazioni del sistema, prevedendo e prevenendo i guasti prima che si verifichino situazioni critiche.
Le informazioni raccolte, condivise e utilizzate, favoriscono una migliore fruizione da parte dell'utente finale, permettono di diminuire i costi e realizzare profitti, consentono lo sviluppo di nuove applicazioni e, più in generale, conferiscono un valore aggiunto alla tecnologia.
Automatizzare e ottimizzare questi benefici attraverso la gestione e il monitoraggio remoti è un'applicazione pratica di notevole rilievo della tecnologia M2M; l'intero comparto embedded potrà trarre vantaggi non indifferenti dalla possibilità di rilevare potenziali problemi prima del loro manifestarsi.

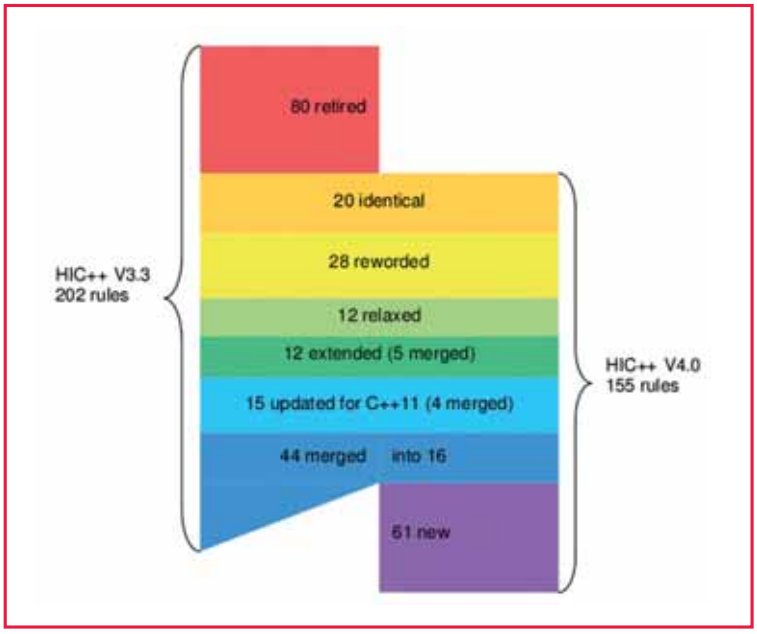
C++: la 'grammatica' per un codice senza errori

II parte*

La complessità di questo linguaggio esige una conoscenza profonda delle regole sintattiche e della semantica, specie quando si sta sviluppando codice per sistemi embedded safety-critical

Giorgio Fusari

Come anticipato nella prima parte di questa mini-guida dedicata a chi intende sviluppare codice di qualità per il mondo embedded, in questo secondo articolo ci si concentrerà sull'uso del linguaggio di programmazione C++. In particolare, si analizzeranno le principali tipologie di standard di codifica, fornendo alcuni consigli e principi base per evitare gli errori classici, e andare verso la produzione di codice il più possibile limpido, comprensibile, corretto, portabile e manutenibile. Caratteristiche, queste, che certamente vanno nella direzione di favorire il lavoro collaborativo negli ambienti e nelle comunità di sviluppatori.



Le variazioni delle regole nello standard di codifica HIC++ V3.3 e V4.0

Già nella prima parte di questo articolo si accennava come il linguaggio C++, nel tempo, sia diventato uno strumento di sviluppo sempre più diffuso e utilizzato dai progettisti di sistemi embedded, anche di tipo safety-critical, e per applicazioni caratterizzate dalla necessità di soddisfare requisiti di funzionamento 'hard real-time'. Una delle ragioni di tale diffusione è legata alla ricchezza semantica di C++, all'elevato livello di astrazione e alla flessibilità che fornisce allo sviluppatore impegnato nella creazione di applicazioni complesse.

Tra i vari benefici, C++ supporta direttamente la programmazione ad oggetti (object oriented), principio progettuale ormai largamente adottato, per i suoi vantaggi nel mondo del software. In aggiunta, la disponibilità sul mercato di strumenti di calcolo tecnico come MATLAB, ampiamente adottati da ingegneri e ricercatori nel mondo industriale e universitario, consente ai diversi sviluppatori di generare in automatico codice C/C++. Ancora, i compilatori C++ sono reperibili per la stragrande maggioranza delle piattaforme hardware, e ciò agevola la portabilità delle applicazioni scritte in questo codice su diverse categorie di processori.

Non proprio adatto ai sistemi safety-critical

Dopo aver enumerato i pro, ora veniamo ai contro del linguaggio C++. La stessa ricchezza semantica, la potenza e il grado di libertà in fase di sviluppo che C++ fornisce all'utente può trasformarsi al contempo nella sua 'debolezza': un'arma a doppio taglio, che esige maggior autodisciplina e capacità di controllo da parte dello stesso sviluppatore. In altri termini, C++ non rappresenta propriamente uno strumento ideale da usare nella progettazione di applicazioni safety-critical, dove il software deve funzionare con estrema affidabilità, in sistemi 'delicati' (sistemi automotive, applicazioni militari, industriali, medicali), in cui un malfunzionamento o un comportamento inatteso del codice può determinare conseguenze anche molto gravi e tragiche. Perché C++ non sarebbe adatto? Perché la natura complessa di questo linguaggio incrementa la probabilità di introdurre nel programma errori che non possono essere identificati e segnalati da un compilatore.
Alcune strutture sintattiche di C++, e la sua semantica, lasciano talvolta spazio ad ambiguità di interpretazione (ad esempio, le ambiguità possibili nella chiamate delle funzioni). Ambiguità che poi, a livello di compilazione, si traducono e si riflettono in variazioni dei comportamenti del programma a seconda del tipo di compilatore utilizzato. Da ciò si deduce l'importanza e la necessità di acquisire una conoscenza più profonda possibile del linguaggio C++, per evitare che la notevole complessità semantica vada a ripercuotersi negativamente sul programma, con l'insorgenza di un maggior numero di errori durante l'attività del compiler. Nello specifico caso dei sistemi embedded che si rivelano critici per la sicurezza fisica – ossia le applicazioni 'safety-critical', dai sistemi avionici, a quelli medicali – occorre evitare quanto più è possibile l'uso di costrutti e forme sintattiche del codice che portino a funzionamenti imprevisti del software.

Standard e linee guida di codifica: i riferimenti chiave

Nel tempo, una strategia indirizzata a ridurre la possibilità di produrre difetti ed errori di programmazione nello sviluppo del codice, con il conseguente manifestarsi di funzionamenti inattesi nel sistema embedded, è stata l'adozione dei cosiddetti standard di codifica. Questi ultimi, in sostanza, puntano a canalizzare e concentrare le funzionalità di C++ entro un insieme più ridotto di caratteristiche e funzioni, che un programmatore può adoperare con una ragionevole sicurezza, senza la preoccupazione di generare errori e inconvenienti di vario tipo nel successivo comportamento del codice creato per una specifica applicazione.
Tra i benefici chiave dell'utilizzo degli standard di codifica non vi è soltanto un incremento della qualità e della manutenibilità del codice: a guadagnarne è anche la velocità di sviluppo, e il lavoro di gruppo, che può essere svolto con maggior efficienza, grazie a una migliorata leggibilità dei programmi.
Nello specifico settore dei sistemi embedded safety-critical, negli anni sono comparsi sulla scena diversi standard di codifica. Tra i più noti c'è, ad esempio, JSF AV C++ (Joint Strike Fighter Air Vehicle C++) - lo standard utilizzato per l'utilizzo di C++ nello sviluppo di software avionico nell'ambito del programma JSF del dipartimento della Difesa Usa. JSF C++ ha mutuato varie regole dal MISRA-C (Motor Industry Software Reliability Association), uno standard di codifica pubblicato per la prima volta nel 1998, rivisto nel 2004, e indirizzato a facilitare l'utilizzo del linguaggio C nello sviluppo di sistemi safety-critical. Tuttavia, la sempre maggiore tendenza a favorire la diffusione e l'adozione di C++ per la progettazione di sistemi safety-critical ha portato alla definizione, nel 2008, dello standard di codifica MISRA-C++.
Un altro standard di codifica che fornisce regole e raccomandazioni per la codifica sicura è lo standard CERT C++. Anch'esso punta all'obiettivo chiave di eliminare le pratiche di codifica inaffidabili e i comportamenti indefiniti del software, che possono portare alla formazione di vulnerabilità sfruttabili. Il principio base è sempre far leva su uno standard di codifica sicuro, in grado di condurre alla creazione di sistemi di più alta qualità, caratterizzati da una maggior robustezza e resistenza ad attacchi e minacce.
Ancora, tra gli standard di codifica per C++, una posizione di rilievo è occupata anche dallo standard High Integrity C++ (HIC++), pubblicato in origine nel 2003 come un insieme di 202 regole e linee guida semantiche e sintattiche, ricavate da un subset 'sicuro' del linguaggio C (ISO C++ 2003). Dopo oltre un decennio di attività, HIC++ ha ricevuto un aggiornamento importante con l'update HIC++ V4.0, rilasciato verso la fine del 2013. Quest'ultimo ha comportato il ritiro di 80 regole per varie ragioni specifiche, con l'obiettivo generale di creare un insieme di regole più applicabile e gestibile.

Principi generali

Prima di passare all'analisi di alcune linee guida specificate dai diversi standard di codifica, vale la pena fornire alcune indicazioni e consigli generali da seguire durante la scrittura del codice. Un primo criterio fondamentale, volto a favorire la leggibilità e chiarezza del codice, è imparare a usare identificatori appropriati.
Un identificatore è una sequenza di caratteri che si usa per definire un elemento del programma: ad esempio, il nome di una variabile, di una funzione, di un oggetto o di una classe. In C++ - che è un linguaggio 'case sensitive',

e fa quindi distinzione fra un carattere maiuscolo e uno minuscolo - gli identificatori sono combinazioni di caratteri alfanumerici, in cui il primo carattere deve essere una lettera dell'alfabeto (maiuscola o minuscola) o un carattere di sottolineatura (underscore '_'), mentre i rimanenti possono essere lettere, cifre o underscore. Negli identificatori, per i nomi non è ammesso utilizzare parole chiave, e nemmeno caratteri speciali. Alcuni esempi di identificatori validi sono:

nome (l'uso di lettere minuscole è consentito)
Cognome (l'uso di lettere maiuscole e minuscole è consentito)
_alpha (l'uso del carattere di sottolineatura all'inizio è permesso)
_SOMMA (l'uso del carattere di sottolineatura all'inizio è permesso anche con lettere maiuscole)
numero_1 (l'uso di underscore e numeri è permesso, assieme alle lettere)
INT (qui l'uso della parola chiave riservata 'int' di C++ è consentito, cambiando però le lettere in maiuscolo)

Esempi di identificatori invalidi, fonte di possibili errori in fase di compilazione, possono invece essere:
int (è una parola chiave riservata di C++)
numero 1 (l'uso degli spazi non è consentito)
8alpha (il primo carattere non è una lettera)
In aggiunta, una nota riguarda la chiarezza dell'identificatore: se da un lato, quando il contesto logico risulta chiaro, l'uso di identificatori brevi e concisi per funzioni e variabili favorisce la sintesi, giovando alla leggibilità, dall'altro, quando il contesto è imprecisato, è consigliabile scrivere identificatori in grado di precisare lo scopo dell'elemento identificato. Quindi adottare, quando il contesto lo richiede, identificatori con un nome più lungo, descrittivo e legato al significato logico ricoperto all'interno del programma: cosa del resto facilitata dal fatto che C++ permette di scrivere nomi anche con un notevole numero di caratteri.
Un'altra indicazione generale che si può fornire è scegliere un'unica lingua – ad esempio quella inglese – utilizzandola nell'intero ciclo di sviluppo del programma. L'uso della lingua italiana può essere consigliabile se il team di progettazione non conosce l'inglese, ma poiché quest'ultima lingua è usata come riferimento nella creazione della stragrande maggioranza delle librerie, l'adozione dell'italiano potrebbe costituire una limitazione non trascurabile per la diffusione, e il riuso del codice in un contesto internazionale di programmazione. Nei vari programmi è anche consigliabile evitare l'uso simultaneo di lingue differenti. Inoltre, la definizione degli identificatori, quindi dei nomi, per le classi e i tipi dovrebbe privilegiare nomi descrittivi, che riflettano la tipologia dei dati. È preferibile un nome che identifichi una rappresentazione astratta della classe, rispetto a una sua implementazione specifica. Nella definizione di funzioni e procedure, è consigliabile che il nome indichi, con un corretto livello di astrazione, ciò che la funzione calcola, o i vari task che la procedura esegue.
Per le variabili, è bene scegliere fin dall'inizio gli identificatori in modo opportuno, tenendo presente che sarà improbabile, in fase di debugging e manutenzione del programma, che verranno cambiati. Qui, analogamente ai discorsi fatti in precedenza, il principio è utilizzare indicatori con nomi brevi nel caso di variabili locali con un uso chiaro nel relativo contesto, e nomi più lunghi e descrittivi per le variabili con un campo di validità globale.

Codice per sistemi critici, i passi falsi da evitare

Quando si utilizza il linguaggio C++ nello sviluppo di un sistema safety-critical, ci sono alcuni specifici aspetti su cui occorre porre particolare attenzione. Qui ne evidenziamo alcuni.
Limitare l'uso del preprocessore. Quando si tratta di sistemi embedded critici per la safety, è bene rispettare alcune limitazioni a cui è soggetto l'utilizzo del preprocessore, ossia il programma che riceve ed esegue le direttive (le righe che iniziano con il carattere #) , producendo codice sorgente per il compilatore. In sostanza, l'uso del preprocessore viene limitato soltanto per l'implementazione delle direttive #include guard, evitando l'uso macro complesse e di inclusioni multiple. Come prescrive lo standard di codifica HIC++, dovrebbero essere utilizzate solo le seguenti forme di direttive #include:

```
• #include <xyz>
• #include "xyz"
```

Fonte PQRA

Ecco poi alcuni esempi di conformità, e non conformità, del codice indicati nelle linee guida HIC++:

```
// Compliant
#include <stddef>

// Non-Compliant
#define MYHEADER "stddef"
#include MYHEADER

// Non-Compliant
#define CPU 1044
#ifndef CPU
#error "no_CPU_defined"
#endif
```

Fonte PQRA

Limitare (o evitare) l'uso dell'allocazione dinamica della memoria. L'utilizzo della memoria dinamica nei sistemi safety-critical è di norma fortemente soggetto a restrizioni, e spesso sconsigliato. Il fondamento logico di questa raccomandazione è che usando l'allocazione dinamica della memoria si aumenta la probabilità che il sistema embedded possa incorrere in bug, e tenda ad assumere un comportamento non deterministico e impredicibile, con impatti sulle performance. L'allocazione statica della memoria consente invece di ottenere un pieno determinismo ed evitare bug di tal genere.

Sintassi per le istruzioni condizionali. Quando si utilizzano le istruzioni if, else, while, for, do e switch, occorre evitare costrutti che possono portare a scrivere codice non valido. Dopo ogni istruzione, ciascun blocco deve essere racchiuso tra parentesi graffe, anche se è vuoto o contiene solo una riga. Ad esempio:

```
#include <cstdint>

void doSomething ();

void foo (int32_t i)
{
  if (0 == i)
    doSomething (); // Non-Compliant
  else
    ;               // Non-Compliant

  if (0 == i)
  {                 // Compliant
    doSomething ();
  }
  else
  {                 // Compliant
  }

  switch (i)
  case 0:
    doSomething (); // Non-Compliant
}
```

Fonte PQRA

Scrivere codice conforme allo standard C++ ISO 2011. Una raccomandazione generale (implementation compliance) riportata nello standard di codifica HIC++ V4.0 spiega che l'attuale versione del linguaggio C++ è quella definita dallo standard internazionale ISO/IEC 14882:2011.
L'osservanza di questo criterio è fondamentale, perché sul mercato esistono compilatori che spesso forniscono funzionalità che oltrepassano quelle definite nello standard sopra citato, e un uso sregolato di tali caratteristiche finirebbe per ostacolare la portabilità del codice.
Adottare tool di automazione della verifica della conformità del codice. Sul mercato esistono vari prodotti e strumenti software in grado di automatizzare l'analisi del codice sorgente, per controllarne e verificarne la conformità secondo le regole definite dalle diverse versioni degli standard di codifica, come ad esempio MISRA-C++ o JSF AV C++.

Evitare il codice implementation-defined, o con comportamento non definito. Un altro criterio essenziale da rispettare è non indirizzarsi verso lo sviluppo di costrutti sintattici e codice, cosiddetto, 'implementation-defined' (definito dall'implementazione), o con un comportamento 'unspecified' (imprecisato) o 'undefined' (non definito).
Infatti, un codice di questo tipo non è portabile e viene bandito dagli standard di codifica. A differenza di un codice conforme allo standard, e compilabile da qualunque compiler fedele agli standard stessi, un costrutto del linguaggio C++, catalogato come implementation-defined, potrà essere implementato a seconda del compilatore in modi differenti, manifestando comportamenti definiti e documentati, con eventuale specifica di quali sono quelli consentiti.
Quando invece il codice è 'unspecified', significa che il comportamento dell'implementazione non è necessariamente documentato.
Infine, il comportamento 'undefined' del codice indica che gli standard non pongono alcun requisito da soddisfare per l'implementazione: quindi il compilatore potrebbe fallire durante la compilazione di porzioni di codice, andare in crash, produrre in modo silente risultati scorretti o, anche, eseguire in maniera fortuita proprio ciò che lo sviluppatore intendeva ottenere.

Naturalmente, in questi pochi punti abbiamo solo evidenziato alcuni aspetti rilevanti che riguardano le migliori pratiche di codifica del codice. Per una trattazione più approfondita e completa è possibile consultare le specifiche linee guida e documenti (ad esempio HIC++) - in alcuni casi scaricabili liberamente online – che raccolgono tutte le principali regole e best practice di programmazione per il linguaggio C++.

Nota
**La prima parte è stata pubblicata sul n. 52-giugno 2014 con il titolo "Software embedded, le linee guida per un codice di qualità"*
Online su http://elettronica-plus.it/brochure/emb/52/#64

La protezione dei sistemi IoT dagli attacchi persistenti

Per individuare gli attacchi informatici più letali come APT e rootkit occorrono hypervisor capaci di filtrare le attività che avvengono fra il sistema operativo e il livello hardware pur rimanendo invisibili sia rispetto all'ambiente ospitante sia nei riguardi delle infezioni che cercano di introdursi

Avishai Ziv
Vice president
Cyber Security Solutions
Lynx Software Technologies

La crescente aspettativa che accompagna il graduale ma inesorabile diffondersi dei sistemi per Internet-of-Things è al tempo stesso uno stimolo per i progettisti e gli sviluppatori alle prese con la preoccupazione dei fornitori di servizi sulla reale possibilità di proteggere i dati e i dispositivi dagli attacchi degli hacker e dai malware circolanti in una rete che sta assumendo dimensioni colossali. Il problema consiste, in pratica, nel personalizzare i contenuti a sufficienza per poterli far viaggiare in rete attraverso infrastrutture standardizzate che hanno la sventura di essere quanto più trasparenti possibile per adattarsi a tutte le tecnologie hardware e software diffuse nel pianeta. Se questo riesce con difficoltà per la protezione dal malware si può solo immaginare quanto sia arduo escogitare tecniche di protezione efficaci contro gli esperti professionisti, che immettono in rete virus o procedure software capaci di carpire informazioni sensibili, piuttosto che danneggiare irrimediabilmente i contenuti critici.
Per questi attacchi è stato coniato l'acronimo di Advanced Persistent Threats, o APT, che li descrive come attività di pirateria informatica svolte nascostamente e persistentemente da esperti che il più delle volte mirano a ben determinati obiettivi con motivazioni economiche o politiche e per raggiungere il loro risultato sono in grado di insistere a lungo impegnando considerevoli risorse. Ciò spiega la denominazione perché Advanced sottintende all'uso di malware sofisticati al punto da essere efficaci nella loro azione distruttiva quanto invisibili alle consuete tecniche di sicurezza antivirus mentre Persistent indica un'attività di monitoraggio sulla rete che può continuare molto a lungo finché non siano catturate le informazioni che interessano e, infine, Threat perché a orchestrare il tutto ci sono persone di grande competenza ed esperienza sulle tecnologie che si utilizzano in rete oltre che ben determinate ad arrivare all'obiettivo, per il quale sono evidentemente e adeguatamente finanziate. Da ciò si capisce perché le attuali tecnologie non sono in grado di accorgersi di questi attacchi e perché occorra sviluppare nuove tecniche di sorveglianza più efficaci ma anche più agili come i Secure Embedded Hypervisor che sono, in pratica, macchine virtuali di monitoraggio capaci di osservare i flussi dati senza alterarli pur cogliendo quegli eventi straordinari che possono essere sintomi di attività di attacco non convenzionali e perciò sfuggenti ai consueti software di protezione. Il problema è che gli attacchi APT possono durare molti mesi a decorrere dalla prima infezione, prima che si possano evidenziare delle anomalie sintomatiche di un'attività piratesca ed è perciò che gli antivirus non servono a nulla ma occorrono strumenti ben più sofisticati come i nuovi Secure Embedded Hypervisor. Precisamente, sono degli algoritmi incapsulati dentro altri sottosistemi e possono funzionare autonomamente e indipendentemente da ciò che succede nell'ambiente dove sono installati così da poter monitorare alcune variabili senza alterarne il flusso dentro i processi principali. Ciò significa che sono permanentemente adattati all'ambiente operativo che li circonda assecondando anche le attività in tempo reale tipiche degli RTOS e le funzioni specifiche di tutti i diversi coprocessori presenti.

Attacchi ben congegnati

Analizzando come si svolge un tipico attacco APT s'identificano tre fasi fondamentali che consistono in una preparazione

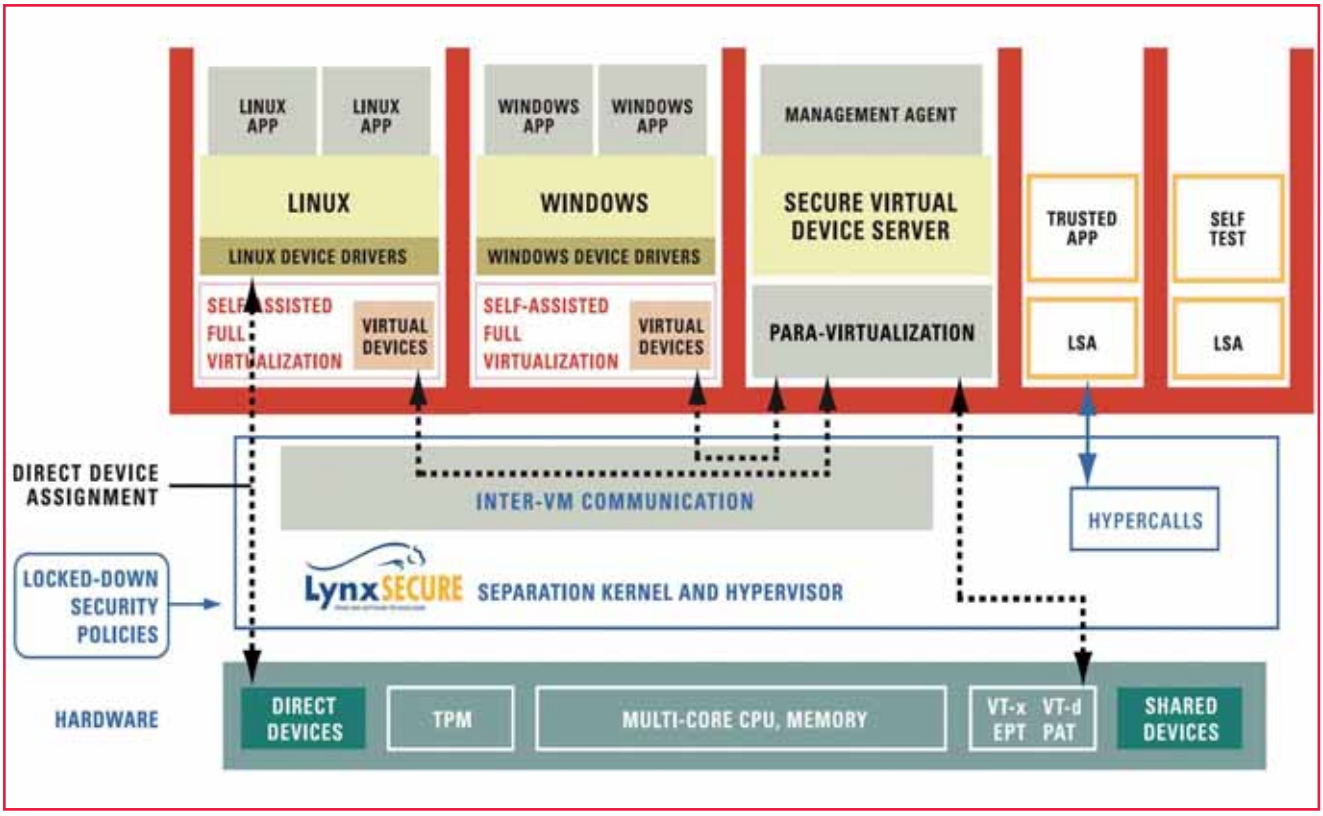


Fig. 1 – Le macchine virtuali di monitoraggio si frappongono tra il livello hardware e il sistema operativo e consentono di individuare gli attacchi APT nel momento in cui cercano di introdurre le infezioni

iniziale basata sull'analisi dell'ambiente da colpire seguita da un'infezione che può avvenire in diversi modi e poi in ultima istanza dall'attacco vero e proprio con l'ottenimento del risultato. La preparazione è fondamentale al pirata per individuare dove l'obiettivo è più vulnerabile e in particolar modo quali siti frequenta maggiormente e da quali preleva più dati che abbiano un discreto margine per permettere l'infiltrazione di esche invisibili. Depositata al posto giusto e nel momento giusto, l'infezione può quindi essere raccolta dall'obiettivo che la inserisce nel proprio sistema dove può rimanere a lungo e preparare il terreno per l'attacco, per esempio, craccando delle password oppure abilitando l'ingresso al sistema attraverso accessi riservati, mentre nel contempo viene raggiunta da altre controparti che la irrobustiscono finché non si palesa il momento opportuno per l'attacco.
Questo poi può manifestarsi con la comunicazione dei dati catturati a un altro sito oppure con la modifica di alcuni dati interni al sistema ospitante o ancora con la distruzione di alcuni registri di sistema o quant'altro.
Attualmente non c'è alcun modo di evitare la prima fase e gli attuali software anti malware riescono seppur faticosamente a fronteggiare la terza quando l'attacco è già in atto bloccandone ogni attività. Sulla seconda fase infettiva si stanno concentrando tutti gli sforzi degli addetti ai lavori perché, in effetti, questa avviene quasi interamente in hardware con passaggi che sfuggono ai software presenti malgrado poi le conseguenze appaiano proprio al livello del sistema operativo quando ormai è troppo tardi. È qui che c'è ancora margine di azione per gli attacchi APT ed è proprio per individuare e fronteggiare le infezioni latenti che si stanno studiando e sperimentando nuove tecniche basate sulle macchine virtuali.

Sicurezza virtuale

In pratica, gli hypervisor devono essere della stessa natura delle infezioni e perciò capaci di monitorare l'ambiente con continuità pur rimanendo invisibili al sistema. Si tratta, dunque, di procedure con priorità più alta delle altre per essere inattaccabili ma con funzionalità di livello abbastanza basso per accorgersi delle infezioni negli algoritmi. Con quest'impostazione è stato realizzato il LynxSecure che viene definito come Separation Kernel Hypervisor (SKH) perché si interpone fra l'hardware e il software creando una scheda madre virtuale che il sistema operativo crede davvero essere quella originale. Si compone, in effetti, di un insieme di algoritmi capaci di identi-

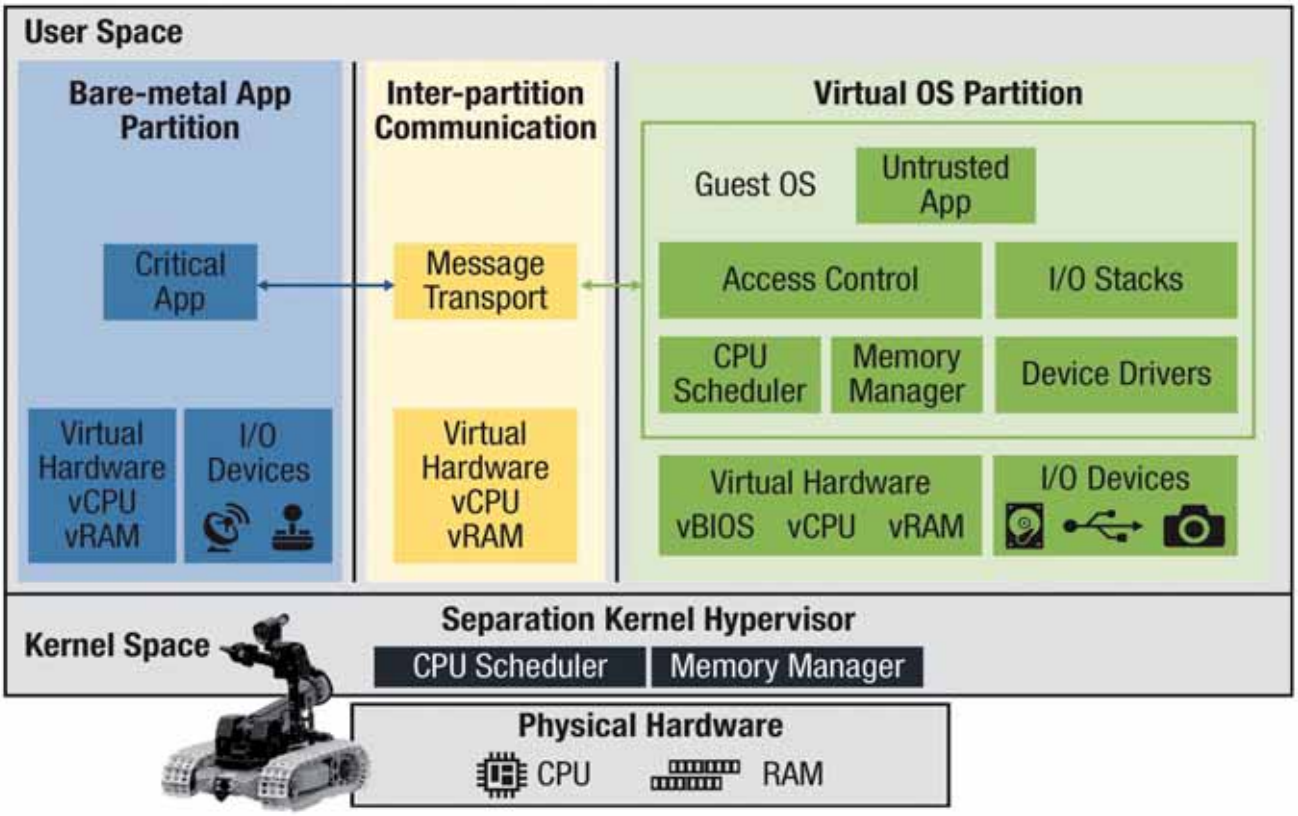


Fig. 2 – Nell'RDS5201 di Lynx Software Technologies c'è l'ultima versione 5.2 del Separation Kernel Hypervisor LynxSecure con più motori di analisi che riescono a catturare anche i letali rootki

ficare i kernel che governano le attività e separarli in funzione del loro dominio di pertinenza analizzandone il flusso dati che li attiene per accorgersi delle probabilità d'infezione. In pratica, sostituisce la gestione delle risorse hardware come memorie, processori e interfacce senza che il sistema operativo se ne accorga e senza che se ne accorgano i processi hardware in modo tale da individuare le anomalie senza intercettarle. La sua azione di filtraggio è efficace perché invisibile sia rispetto al sistema operativo presente sia nei confronti delle infezioni che cercano di entrare. S
e così non fosse rischierebbe di diventare un'arma a doppio taglio per i pirati che potrebbero servirsene per rendere più deleterio il processo infettivo. La sua efficacia è dovuta ai tanti piccoli motori in grado di monitorare i parametri più critici del sistema senza modificarli in modo da consentire poi a un software di analisi esterno di individuare le probabili infezioni. Questo genere di analisi, infatti, può durare mesi perché tanto durano le infezioni e perciò occorrono software specificatamente sviluppati a tal scopo e implementati in PC isolati e a loro volta adeguatamente protetti dai malware e dagli APT.
LynuxWorks ha cambiato il nome quest'estate in Lynx Software Technologies continuando con questo marchio a distribuire i suoi prodotti principali che sono il sistema operativo LynxOS e il kernel LynxSecure. Fra le più recenti novità presentate dalla società londinese c'è l'innovativo Rootkit Detection System RDS5201 che consente di individuare i peggiori fra gli attacchi APT e cioè i "rootkit" capaci di insediarsi al punto di ottenere il controllo di un sistema a prescindere dall'autorizzazione dell'amministratore.
I più celebri e nefasti sono noti come "cavalli di Troia" ma se ne conoscono anche di benevoli come, per esempio, il rootkit introdotto da Sony per prevenire l'accesso del malware nelle PlayStation 3. I più attuali sono veri e propri kernel che riescono a emulare i livelli più privilegiati dei sistemi operativi e modificare i registri a livello di sistema. Per questi attacchi è necessaria un'osservazione particolarmente mirata con più motori di monitoraggio capaci di agire contemporaneamente. L'RDS5201 ospita l'ultima versione dell'hypervisor LynxSecure 5.2 che integra meccanismi antivirus tradizionali insieme ad algoritmi capaci di eseguire analisi multiple sui flussi di dati e accorgersi della presenza delle infiltrazioni probabilmente infettive in pochi minuti senza bisogno di ricorrere a software dedicati che per la stessa funzione hanno bisogno di settimane o mesi di attesa.

RTOS, l'evoluzione della specie

Trasformazioni globali come la IoT (Internet of Things) ridisegnano il ruolo dei sistemi operativi real-time, elevandone i requisiti tecnologici

Giorgio Fusari

Attualmente formano un mercato ancora frammentato, costellato da una grande varietà di soluzioni disponibili. Ma con il tempo sono divenuti sempre più sofisticati e strategici per il funzionamento di molte nuove applicazioni embedded: i sistemi operativi real-time (real-time operating system – RTOS) appartengono a un settore di sviluppo del software che, come altri, ha dovuto necessariamente fare i conti con i profondi cambiamenti avvenuti nello spazio della tecnologia elettronica in questi anni.

Guardando un po' indietro, e osservando la strada percorsa e lasciata alle spalle dal progresso tecnologico, si comprende meglio il valore del contenuto d'innovazione racchiuso negli attuali RTOS. Ci si accorge anche di quanto essi non siano più da tempo semplicemente classificabili come soluzioni software di utilizzo tipico nei classici domini industriali. Sistemi con un funzionamento generalmente ascrivibile agli ambienti di fabbrica, o ad applicazioni con stringenti vincoli di affidabilità nell'esecuzione dei task, nella gestione della memoria, e nel funzionamento deterministico.

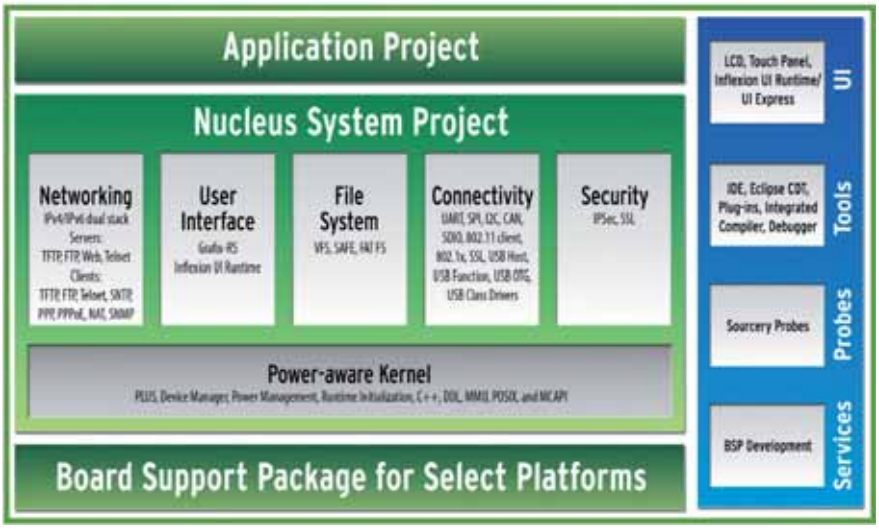


Fig. 1 – L'architettura di Nucleus, il sistema operativo real-time di Mentor Graphics

Al principio, in passato, le attività di sviluppo dei fornitori di sistemi operativi embedded hanno tradizionalmente dovuto spesso misurarsi con le difficoltà d'implementazione mostrate da OEM e costruttori di dispositivi nei vari progetti. E tenere conto, nell'aggiunta delle nuove funzionalità, dell'esistenza di hardware embedded con risorse limitate (processore, memoria, interfacce di connettività e così via), oltre che dei vincoli di costi e di tempo da rispettare nella realizzazione delle applicazioni.

Con 'IoT' arrivano nuove sfide

Gli RTOS stanno evolvendosi per sopravvivere in un panorama tecnologico che si è velocemente allargato, dive-

nendo molto più complesso. Oggi trasformazioni globali come il cloud computing o la Internet degli oggetti (IoT – Internet of Things) fanno sì che i sistemi embedded non siano più mere isole tecnologiche a se stanti e scollegate dal network, ma si possano ritrovare diffusi capillarmente in molti più ambienti e applicazioni: si parla in prospettiva di miliardi di dispositivi embedded connessi stabilmente all'infrastruttura IT.
Inoltre, nel frattempo, lo sviluppo dell'elettronica embedded ha reso disponibili architetture hardware molto più potenti e complesse, caratterizzate da system-on-chip (SoC) multicore, dotati di una capacità di calcolo parallelo che però richiede di essere adeguatamente controllata e sfruttata in maniera efficiente grazie all'intelligenza del software.
Oggi, dalla periferia della rete, i vari oggetti e dispositivi intelligenti connessi al cloud e all'IoT sono in grado di comunicare con i sistemi di back-end aziendali, fornendo enormi moli di informazioni. Big Data che, una volta raccolti ed elaborati in tempo reale da sistemi analitici e di business intelligence, permettono di migliorare con dinamicità prodotti e servizi, o gestire macchinari industriali e infrastrutture di pubblica utilità con maggiore efficienza.
Ma tutto ciò richiede RTOS con caratteristiche tecnologiche e funzionalità adeguate.
Nel tempo, molti fornitori di sistemi operativi sono gradualmente migrati da una strategia di offerta basata su semplici prodotti, verso la fornitura di soluzioni complete e ottimizzate, in grado di includere non solo il sistema operativo, ma anche strumenti di sviluppo, oltre ad altri componenti software e servizi di supporto professionale.
Tutti fattori che hanno assunto un ruolo determinante per facilitare l'integrazione degli RTOS nelle varie generazioni di dispositivi embedded.
Oggi, gli intensi cambiamenti tecnologici in corso, e la convergenza nel cloud di molti device dotati di un'intelligenza crescente, complicano ulteriormente la progettazione dei nuovi sistemi operativi, perché le caratteristiche

Linux 'reloaded': alla conquista dello spazio 'real-time'

Molti tentativi di utilizzo di Linux e delle piattaforme Linux-based in diverse applicazioni embedded hanno spesso tradizionalmente incontrato una principale barriera: la difficoltà intrinseca nel sistema di soddisfare i requisiti di funzionamento deterministico e real-time, a cui molti di questi dispositivi devono invece ottemperare. In tali casi, infatti, spesso il sistema deve eseguire con un certo livello di determinismo lo scheduling, il controllo o l'allocazione delle risorse hardware: tutte funzionalità per cui gli RTOS tradizionali, di natura proprietaria, sono stati concepiti, e grazie alle quali riescono ancora a dominare il mercato.
Tuttavia oggi questo scenario sta gradualmente mutando, e riaccendendo il dibattito sulla rivalutazione di Linux.
Attualmente, infatti, il Pinguino sta evolvendosi anche da questo punto di vista, e trasformandosi in una soluzione applicabile nei sistemi embedded che hanno requisiti spesso definiti 'soft real-time', ossia specifiche di funzionamento deterministico non estremamente rigide, a differenza invece di altri sistemi embedded (hard real-time). Secondo alcune molto recenti analisi e considerazioni della società di ricerche VDC Research, una soluzione in prospettiva interessante da questo punto di vista – e quindi in grado di abilitare capacità real-time in Linux embedded – è PREEMPT_RT, una patch real-time per il kernel Linux. Quest'ultima non solo è in grado di migliorare i tempi di risposta del sistema, ma soprattutto di rimuovere tutte le cosiddette 'unbounded latencies', le latenze impredicibili che possono manifestarsi usando il kernel originario (kernel vanilla o mainline kernel). Quando potenziato con PREEMPT_RT, Linux embedded può diventare compatibile per l'utilizzo in applicazioni soft real-time che spaziano dal settore industriale, ai sistemi di automazione nel mondo retail e dell'ufficio, e andare a sostituire gli RTOS tradizionali. Rispetto ad altre soluzioni possibili (ad esempio l'adozione di un hypervisor commerciale in grado, tramite la tecnologia di virtualizzazione, di ospitare sullo stesso sistema, in partizioni separate, Linux e un RTOS), stima VDC, l'uso della patch real-time PREEMP_RT costituisce il modo più immediato per abilitare prestazioni real-time nei sistemi che funzionano con piattaforme Linux-based. Ciò non toglie, tuttavia, la necessità di eseguire ulteriori interventi di sintonizzazione e ottimizzazione sulla piattaforma Linux embedded potenziata con la patch real-time.

architetturali e funzionalità che gli RTOS moderni devono saper integrare sono numerose e sofisticate, e pongono nuove sfide di sviluppo.

Requisiti da soddisfare, non solo determinismo

L'evoluzione degli RTOS verso nuovi, moderni sistemi operativi real-time passa attraverso alcune 'capability' chiave, senza le quali sarebbe oggi impossibile immaginarli. Nel mondo IoT e M2M (machine-to-machine), i dispositivi 'edge' connessi alla periferia della rete possono essere i più vari e, pertanto, caratterizzarsi per capacità e funzionalità anche molto differenti. Tuttavia questi device sono anche accomunati dalla necessità di soddisfare alcuni requisiti indispensabili: primo fra tutti, un funzionamento deterministico, che richiede l'adozione di un RTOS: solo i sistemi operativi di questa categoria sono infatti in grado di assicurare un'operatività capace di rispettare i più o meno rigidi vincoli di timing di queste applicazioni, nonché, quando si rivela necessario, anche severe specifiche di safety.

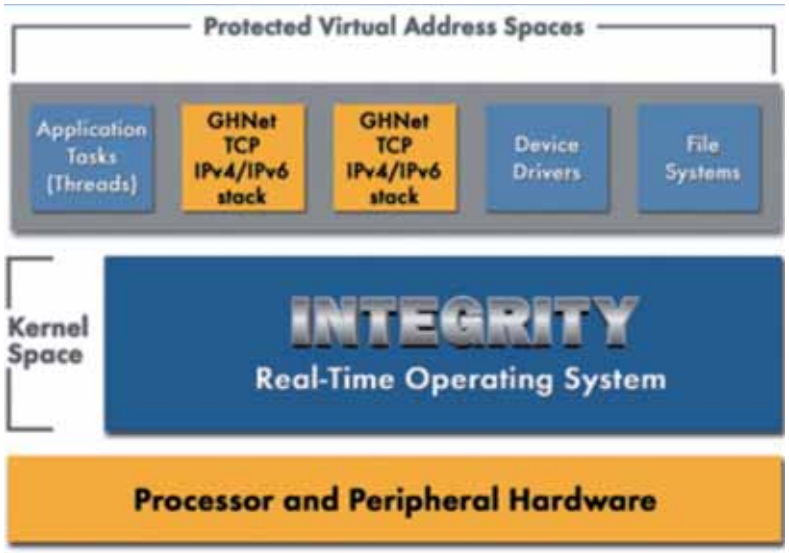


Fig. 2 – Integrity, un RTOS con prestazioni hard real-time

Un altro requisito il cui ruolo è certamente in crescita negli RTOS moderni è la sicurezza. Proprio perché tutti questi nuovi oggetti e sistemi embedded intelligenti si trovano connessi in maniera sempre più capillare nella rete, essi di fatto moltiplicano i potenziali punti di vulnerabilità e le possibilità di attacco informatico a cui è esposta l'infrastruttura. Ma qui non si tratta semplicemente di proteggere il sistema embedded dalle insidie di malware o applicazioni pericolose: il problema è anche dispiegare in rete oggetti e dispositivi edge con a bordo un RTOS che, una volta connessi all'IoT, sia in grado di memorizzare e trasmettere i dati senza subire violazioni di sorta. Un caso tipico, ad esempio, può essere quello di un 'sensor hub' che raccoglie e concentra al proprio interno i dati provenienti da numerosi sensori. A questo livello è essenziale che l'RTOS del dispositivo possieda l'intelligenza necessaria per analizzare tali pacchetti di dati, e verificarne l'integrità, quindi l'assenza di manomissioni. Per eseguire tali operazioni in modo affidabile nel tempo, l'RTOS deve anche essere mantenuto aggiornato tramite periodici upgrade delle funzionalità di security, e utilizzare i meccanismi di autenticazione per la connessione alle varie applicazioni.

I requisiti di safety, cioè di sicurezza fisica, sono richiesti invece soprattutto nelle applicazioni dove un malfunzionamento del sistema operativo che comanda una macchina embedded ha il potenziale di causare il ferimento o addirittura la morte dell'utente. L'RTOS deve quindi essere certificato secondo le specifiche normative di safety dei singoli ambiti operativi.

Imperativo modulare

Nell'era IoT, la modularità del sistema diventa un'altra caratteristica importante. In passato gli RTOS sono stati essenzialmente sistemi monolitici, integrabili di volta in volta nell'hardware target con l'ausilio di un corredo di strumenti di sviluppo, di BSP (board support package) o di altro software middleware. E quando era necessario aggiornarli, ciò avveniva soprattutto per correggere bug di funzionamento o tappare falle di sicurezza. Tutto questo oggi nel mondo cloud risulta impensabile: i dispositivi embedded e i sistemi operativi moderni devono potersi aggiornare di continuo con nuovi componenti, per stare al passo con l'evoluzione della rete. Devono dunque fondarsi su un'architettura modulare, in grado di consentire l'aggiunta di nuove funzionalità, applicazioni, protocolli, middleware o pacchetti, senza dover modificare il kernel, ossia il nucleo centrale dell'RTOS. In questo modo diventa possibile anche allungare il ciclo di vita del sistema operativo, spalmandolo su più generazioni di dispositivi.

Altra caratteristica chiave è la scalabilità. La presenza nell'IoT di una miriade di dispositivi differenti, in termini di dimensioni, potenza e capacità di elaborazione, rende indispensabile per un RTOS odierno l'abilità di scalare l'occupazione di memoria (memory footprint), le funzionalità e le prestazioni di processing in funzione delle singole tipologie di device intelligenti.

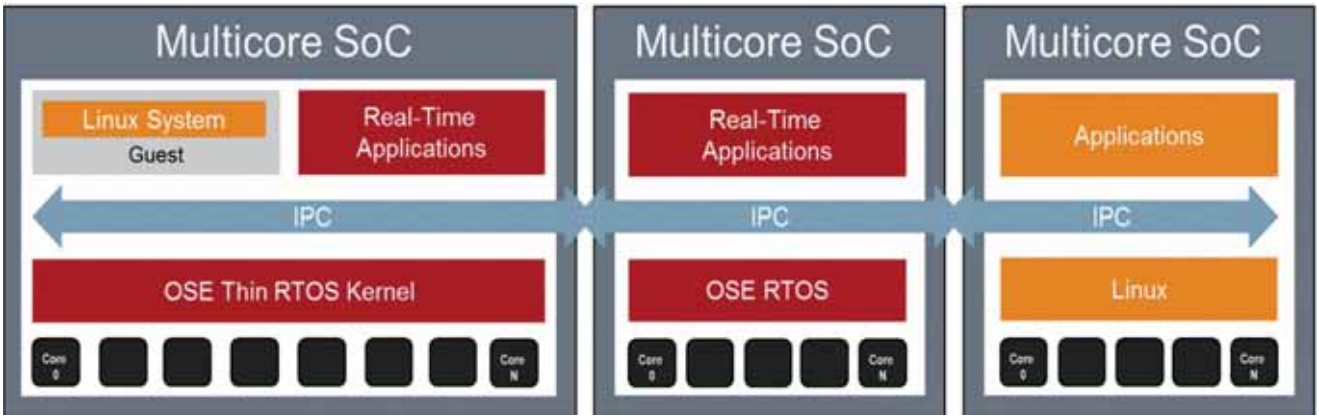


Fig. 3 – Il supporto multicore in Enea OSE permette la coesistenza del RTOS con Linux

Non meno importante è poi la connettività. Con l'avvento e lo sviluppo della IoT, un numero sempre maggiore di dispositivi embedded non risulta più isolato e relegato ad attività tipiche dell'ambito industriale e di fabbrica. Le reti di sensori, spesso formate da dispositivi in grado di comunicare fra loro e con il Web in modalità wireless, sono presenti negli ambiti applicativi più disparati: dai sistemi di monitoraggio e controllo delle colture agricole, ai sistemi di controllo industriali, ai dispositivi medicali per la cura in remoto dei pazienti, in grado di spedire dati diagnostici alle strutture ospedaliere. Di conseguenza, gli attuali RTOS devono soddisfare anche il requisito di supportare tutti i principali standard e protocolli di comunicazione – da Ethernet, a Wi-Fi, a Bluetooth, e quant'altro – integrando nativamente tutte le necessarie funzionalità di networking.

Gli RTOS stanno evolvendosi per sopravvivere in un panorama tecnologico che si è velocemente allargato, divenendo molto più complesso

Altro 'must', differenziare i prodotti

Vi sono poi ulteriori caratteristiche che vanno a completare il profilo di un RTOS di nuova generazione. Fra queste c'è ad esempio la flessibilità dell'interfaccia grafica, che assieme alla modularità del sistema, è molto importante per riuscire a differenziare le funzionalità dei diversi prodotti, specie in un mercato in cui si spazia da dispositivi che possono andare dagli smartphone e tablet, ai device medicali, ai sistemi di controllo industriale. Qui la qualità dell'interfaccia uomo-macchina non si basa solo su motori grafici 2De 3D, ma anche sulla capacità di abilitare le più moderne modalità d'interazione con l'utente, come gli schermi a sfioramento (touchscreen).

Ancora, sempre più, nel quadro di evoluzione degli RTOS, diventa critico per i fornitori di sistemi operativi mettere a disposizione dei costruttori di dispositivi un sistema che, oltre a tutte le caratteristiche precedentemente sottolineate, integra già in modo nativo, 'out-of-the-box', le funzionalità software specifiche indispensabili per operare nel particolare mercato verticale a cui viene indirizzato. In altre parole, un RTOS progettato per il mondo delle applicazioni industriali dovrebbe già fornire agli OEM driver, protocolli, e tutto il necessario software middleware specifico per l'ambiente di fabbrica, in modo da velocizzare le implementazioni sui rispettivi device e ridurre il time-to-market necessario per il rilascio dei prodotti sul mercato. Allo stesso modo, un RTOS personalizzato per il settore medicale dovrebbe disporre già di funzionalità e caratteristiche che lo rendano adatto al funzionamento in conformità con gli specifici requisiti e normative di safety vigenti in un determinato paese.

Richiamando i trend di evoluzione tecnologica citati al principio, non si può nemmeno dimenticare la capacità richiesta ai moderni RTOS di fornire il supporto software per un funzionamento efficiente del sistema operativo e delle applicazioni anche su architetture hardware di tipo multicore, e su processori a 64 bit, che stanno emergendo in modo crescente come piattaforme di riferimento. Altra caratteristica sempre più rilevante, nel quadro di progressiva espansione dell'uso delle piattaforme hardware multicore, è la tecnologia di virtualizzazione. Quest'ultima, grazie ai software hypervisor, permette di consolidare molteplici piattaforme hardware su un singolo sistema multicore in grado di far funzionare diversi sistemi operativi e applicazioni, anche con requisiti real-time.

SO embedded nell'era IoT, fra tradizione ed evoluzione

Le emergenti applicazioni della Internet of Things accrescono il numero di sistemi embedded interconnessi in domini critici. In tali ambiti, i sistemi operativi, per preservare la classica affidabilità, devono rafforzare i meccanismi di sicurezza e protezione dalle minacce della rete

Stefano Rinaldi

Fino a ieri, si potevano considerare 'sistemi embedded critici' soprattutto certe applicazioni confinate in ambito industriale, avionico, militare, automotive, medicale. Applicazioni caratterizzate, naturalmente, da diversi livelli di criticità. Oggi questi confini stanno allargandosi a vista d'occhio a molti altri sistemi embedded, sospinti dall'effetto 'legante' della Internet delle cose. Ma prima di entrare nel merito di quali caratteristiche e requisiti tecnici siano attualmente richiesti ai sistemi operativi e RTOS (real-time operating system) per applicazioni embedded critiche, è utile richiamare lo scenario di trasformazione tecnologica in cui questi SO devono oggi sapersi adattare e operare.

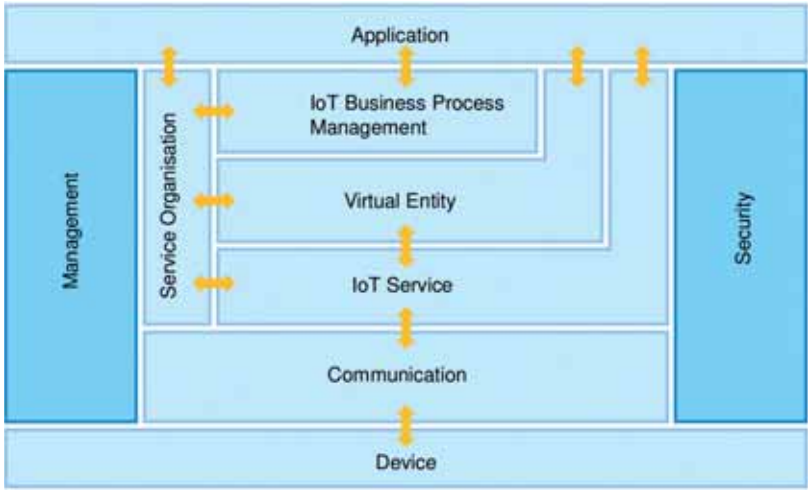


Fig. 1 – Il modello funzionale della Internet of Things

Il mondo 'industrial' entra nel cloud

In maniera analoga a come il cloud computing sta unificando l'IT – facendo convergere data center, computer, dispositivi mobili e altri endopoint verso il paradigma della Nuvola – così la IoT (Internet of Things) è un modello architetturale di IT che sta portando molti dispositivi industriali, prima isolati, nel cloud. Di esempi ve ne sono parecchi.

Si va dai contatori intelligenti (smart meter), alle appliance adottate dalle società di utility per attuare un controllo intelligente sui consumi di energia e sulle bollette degli utenti; dalle telecamere di videosorveglianza installate in imprese, supermercati e abitazioni, alle sempre più pervasive reti di sensori; dai display informativi di pubblica utilità, a molto altro.

Con la diffusione della IoT, il modello as-a-service sta di fatto conquistando anche il mondo industriale, che si ap-

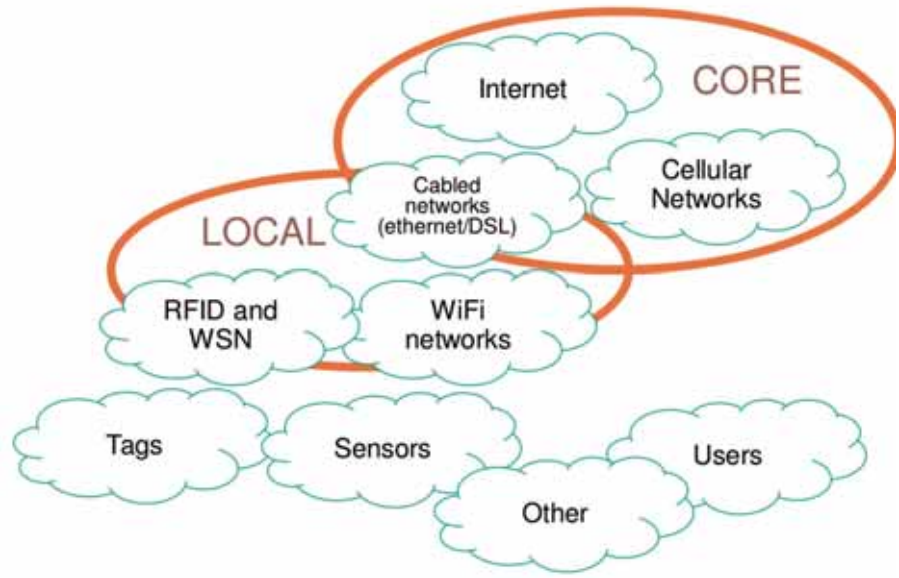


Fig. 2 – La natura eterogenea delle infrastrutture di comunicazione nell'attuale architettura IoT

presta a seguire, in un certo senso, le stesse orme di quello IT. GE (General Electric), ad esempio, una lunga storia nei macchinari e dispositivi industriali, oggi sta cavalcando il trend dell'Industrial Internet e dei Big Data, con l'obiettivo di creare reti di macchine intelligenti che convergono nel cloud, producendo grandi quantità di dati. Questi ultimi sono utilizzabili da una piattaforma di 'asset performance management' (Predix), implementabile on-premise o in cloud privato o pubblico, per ottimizzare l'operatività delle infrastrutture industriali, attraverso servizi analitici e di manutenzione predittiva.
Tutto ciò fa sì che il risultato sia un numero crescente di applicazioni embedded industriali sempre più interconnesse in rete con applicazioni commerciali, per fornire nuove tipologie di servizi. Dunque un contesto di sistemi 'ibridati', che aprono nuovi potenziali punti di vulnerabilità agli attacchi informatici, e da progettare con rinnovati concetti di sicurezza, ispirati all'attuale realtà. Fra l'altro, in un mondo di sistemi embedded interconnessi con applicazioni commerciali di vario tipo, le conseguenze di un malfunzionamento, di un'interruzione o di una compromissione dei servizi possono ripercuotersi in maniera ancora più estesa sugli utenti finali.

Applicazioni interconnesse e nuove sfide

Tutti questi nuovi sistemi embedded distribuiti e applicazioni M2M con operatività critica, immersi e connessi 24 ore su 24 nell'Internet degli oggetti, necessitano di sistemi operativi certamente robusti e affidabili, ma anche dotati di nuove caratteristiche e funzionalità. Da un lato, rimangono sempre validi i criteri chiave, secondo cui le peculiarità di un sistema operativo embedded, e in particolare di un RTOS, risiedono in un footprint contenuto, in affidabilità ed efficienza; in un'accurata gestione delle risorse di memoria e di I/O; nella precisa prioritizzazione dei task in esecuzione, nel controllo degli interrupt, e nella minimizzazione delle latenze, con l'obiettivo di perseguire un comportamento deterministico. Ma sempre più, l'emergente realtà delle poliedriche applicazioni embedded IoT interconnesse pone l'accento su altri requisiti: ad esempio, la dotazione del sistema a livello di connettività e networking; di funzionalità grafiche, di meccanismi di protezione e cybersecurity, di funzionalità di virtualizzazione delle risorse, di gestione dell'energia, di capacità del SO di evolversi in rapporto a necessità di business dinamiche.
Il mondo IoT pone ai sistemi critici interconnessi nuove sfide, in termini di rischi di sicurezza informatica, di flessibilità di adattamento, di durata del ciclo di vita dei prodotti, di costi di sviluppo. Senza contare che in questi ultimi anni le quantità di dati in gioco, le frequenze di elaborazione, le velocità di trasporto delle informazioni, sono enormemente aumentate rispetto al passato. Lo sviluppo e la diffusione di SoC (system-on-chip) con architetture multicore eterogenee (CPU, GPU, DSP e così via) ha generato l'esigenza di gestire sistemi con tecnologie di elaborazione parallela, e con un'attenzione specifica all'efficienza delle comunicazioni interprocesso (IPC).

Requisiti, ancora più critici

La natura costantemente interconnessa e interattiva delle applicazioni IoT, soprattutto quando i servizi e le funzionalità sono critici, richiede ai moderni RTOS embedded elevata affidabilità di funzionamento, ampia capacità di comunicazione in rete, e anche una robustezza superiore, in termini di security e safety.

Spazi di elaborazione protetti. Una caratteristica chiave da porre in rilievo negli RTOS per applicazioni embedded critiche è ad esempio la capacità di alcuni sistemi operativi, nativa o ottenibile tramite hypervisor, di creare zone,

container, sottosistemi, spazi di elaborazione partizionati, e isolati gli uni dagli altri, in cui possono girare diversi SO. Ciascun sottosistema dispone di una certa quantità di memoria allocata e protetta, di risorse di elaborazione e di I/O. Attraverso un'architettura di questo tipo, l'obiettivo è assicurare che il software e i processi che girano in una zona non condizionino il funzionamento e le prestazioni del software e dei processi attivi in un'altra. E soprattutto che il malfunzionamento o il crash dei processi di un sottosistema non provochi l'arresto del software che gira negli altri container.
Grazie a queste caratteristiche, il concetto di consolidamento in uno stesso apparato di diverse applicazioni e sistemi, più o meno critici, può trasformarsi in realtà. Un concetto che da un lato risponde all'esigenza di soddisfare i crescenti requisiti SWaP (size, weight and power) richiesti alle varie applicazioni embedded o 'deeply embedded' e, dall'altro, alla necessità di evitare il più possibile la lievitazione di costi che deriverebbe dall'acquisizione e manutenzione di piattaforme separate.
Inoltre, sulla stessa piattaforma, sistemi real-time con diverso grado di criticità (hard-real-time, o soft-real-time) sono in grado di girare accanto a sistemi e applicazioni non real-time, senza rischiare che un'avaria nel funzionamento di queste ultime possa compromettere l'operatività delle prime.
I vantaggi di tale approccio si possono riscontrare in diverse applicazioni e casi d'uso. Ad esempio, in un'automobile, il medesimo sistema operativo, su un solo apparato, diventa in grado di gestire sia le funzionalità safety-critical (controllo motore, stabilità, impianto frenante e così via), sia l'impianto di infotainment. Lo stesso può valere per un aereo di linea, in cui un solo sistema operativo embedded può amministrare sia i sistemi e i processi di controllo del volo, sia la distribuzione dei programmi e contenuti di intrattenimento per i passeggeri, naturalmente isolandoli in spazi e ambienti di elaborazione separati e protetti.

Sicurezza di rete contro safety. In ambito medicale, industriale, automotive o avionico, i requisiti di safety del SO servono a garantire il mantenimento della sicurezza fisica per le applicazioni, impedendo che malfunzionamenti del software causino lesioni o addirittura la morte dell'utente. I sistemi operativi e il software embedded safety-critical vengono tradizionalmente sottoposti a lunghi e scrupolosi processi di validazione, e possono ottenere diversi livelli di certificazione, ciascuno atto a garantire determinate funzionalità (ARINC 653, DO-178 Level A, DO-178 Level B e così via). Il problema però è che con applicazioni IoT sempre più interconnesse, aumentano i casi d'uso in cui questi sistemi critici finiscono per interagire in modo indefinito e imprevedibile con dispositivi e applicazioni che non sempre hanno seguito lo stesso, severo percorso di regolamentazione e certificazione.
La realtà è, ad esempio, che oggi i costruttori del mondo automotive devono 'difendersi' dall'ingresso dirompente nell'autovettura di dispositivi di elettronica di consumo di varia natura (smartphone, lettori mp3, console videogiochi e così via). È vero, come prima accennato, che esiste un netta linea di demarcazione fra l'ambiente software di entertainment e quello dei sistemi critici (freni, sterzo, controllo stabilità vettura), ma è anche vero che fra i due ambienti vi sono pur sempre connessioni fisiche. Fra l'altro, per rispondere alla domanda di maggior connettività e multimedialità da parte dei consumatori, in questi anni i car maker hanno arricchito diverse categorie di veicoli con funzionalità Wi-Fi, Bluetooth o connessione a reti cellulari. E queste feature possono rappresentare potenziali punti di debolezza e d'ingresso per attacchi di hacking.
Un altro esempio è la proliferazione di accessori e apparecchi medicali indossabili (pulsossimetri, cardiofrequenzimetri, holter wearable) collegabili in modalità wireless a smartphone o tablet, unita alla diffusione di altri dispositivi

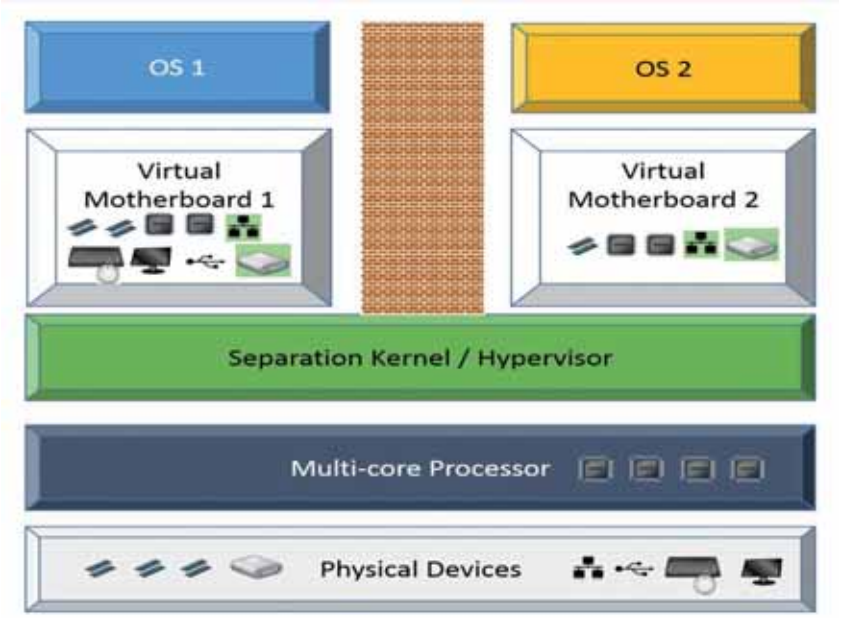


Fig. 3 – Uno schema delle tecnologie di separation kernel e hypervisor in un SO per applicazioni embedded critiche

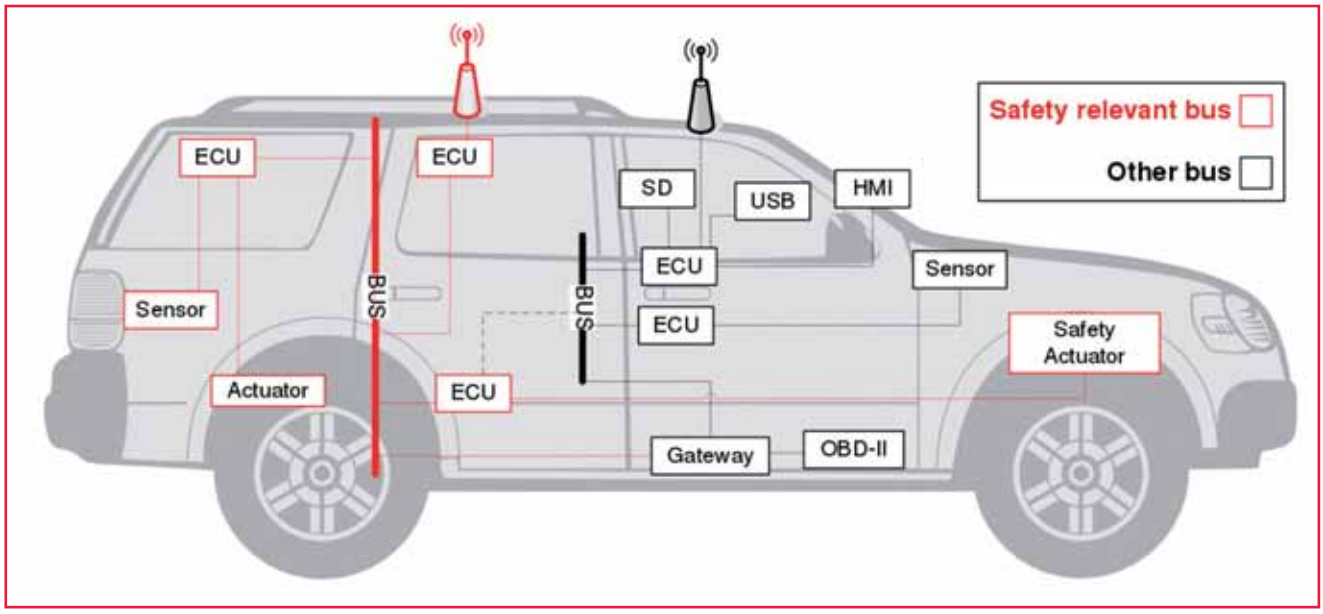


Fig. 4 – Un esempio di applicazione IoT in cui la safety del veicolo può essere messa a rischio da una debolezza nella security. Nel disegno, viene mostrata la connessione fisica esistente tra il bus che presiede alle funzionalità di infotainment (rete cellulare, connessione USB, interfaccia HMI e così via) e il bus che controlla i componenti safety-critical di trasmissione del veicolo

medicali che funzionano come gateway fra i sensori IoT che raccolgono i dati fisiologici del paziente, per poi trasmetterli allo smartphone o al personale sanitario. È anche ben noto, attraverso varie ricerche e studi di mercato, quanto il malware, e il codice infetto colpiscano i dispositivi mobile, specie quelli basati su piattaforma Android e relative app, aprendo falle e problemi di sicurezza. Risulta dunque evidente come nel mondo IoT safety e security siano molto più strettamente legate, e come la fragilità della cybersecurity, della sicurezza di rete di alcuni di questi nuovi componenti possa mettere a rischio anche l'operatività dei sistemi medicali safety-critical. In prospettiva diventa di conseguenza sempre più imperativo per sviluppatori e vendor di sistemi operativi e dispositivi arrivare a soddisfare e garantire i requisiti di safety e security anche per queste emergenti tipologie di sistemi interconnessi.

Modularità e scalabilità. All'inizio del loro percorso nello spazio embedded, gli RTOS potevano 'permettersi' di essere soluzioni con un'architettura di tipo monolitico e non facilmente espandibile tramite l'implementazione di nuove funzionalità. Ora invece, per assecondare le attuali esigenze del mercato e consentire ai costruttori un'agevole e rapida differenziazione dei prodotti, l'architettura preferibile è costituita da una solida struttura portante (core) a cui deve essere possibile aggiungere, in maniera modulare e senza difficoltà di sviluppo, tutti i componenti di volta in volta necessari (nuovi protocolli di networking, software, middleware e così via) per realizzare l'applicazione. In aggiunta, la scalabilità del sistema acquista importanza per la necessità crescente dei costruttori di adattarlo a un'ampia gamma di prodotti e dispositivi embedded: da quelli semplici e quelli più complessi; da quelli con requisiti molto stringenti in termini di risorse hardware disponibili, a quelli maggiormente dotati e potenti.

Capacità di comunicazione. Il megatrend dell'Internet degli oggetti ha oggi trasformato gli RTOS, da sistemi fondamentalmente isolati nel proprio ristretto spazio di operatività, ad esempio in ambienti industriali, a sistemi sempre più interconnessi, non solo con le infrastrutture di produzione, ma anche con le reti private aziendali e le infrastrutture cloud pubbliche. Dunque il nuovo bagaglio di funzionalità dei sistemi operativi per applicazioni critiche deve anche arricchirsi attraverso un maggior assortimento di protocolli e tecnologie di comunicazione, sia di tipo wired, sia wireless (Ethernet, connessioni DSL, WiFi, reti cellulari, RFID, reti di sensori wireless e così via).
Per concludere, l'Internet degli oggetti sta divenendo una realtà sempre più grande. Il convergere dei sistemi embedded nell'IoT amplia i confini e le sfide tecnologiche che sviluppatori e produttori di software devono saper vincere, per continuare a fornire sistemi operativi all'altezza di costituire la base per le applicazioni di nuova generazione.

COM per applicazioni militari

Advantech ha presentato moduli COM per applicazioni militari, dotati di robustezza, flessibilità e facilità di progettazione, che offrono soluzioni facilmente scalabili.
La robustezza dei moduli, il know-how sicuro e i servizi di progettazione, rendono i moduli COM una misura ideale per applicazioni militari.
La creazione di soluzioni rugged richiede

una combinazione di buon design, buoni componenti, buona progettazione e tanti test in più. L'approccio di Advantech alla progettazione integrata per il funzionamento in ambiente estremo, comprende un'ampia gamma di test di temperatura, soluzioni sofisticate, servizi di consulenza e varie prove di vibrazione.

Mini modulo COM Express con supporto ECC

Congatec ha realizzato un mini modulo COM Express (conga-MA3E) con supporto ECC (Error Correction Code), basato sulla serie di processori Intel Atom E3800. Diversamente dai moduli standard RAM, i moduli ECC presentano funzioni aggiuntive per controllare il flusso di dati e correggere errori. Sia conga-MA3 sia conga-MA3E presentano l'ultimo design Intel Atom, una cache L2 in grado di essere condivisa da più core, e un motore grafico HD molto più veloce di Intel rispetto alla generazione precedente. Altri punti salienti dei moduli includono un design ultra-denso, memoria DDR3L (ECC per la conga-MA3E) con supporto fino a 8GBytes. Entrambi i moduli supportano le versioni di temperatura nominale commerciali e industriali che vanno dalla entry-level single-core al quad-core Intel Atom E3845 con 1.91 GHz e 10 watt di consumo di potenza massima. La grafica migliorata supporta DirectX 11, OpenGL 3.2 e OpenCL 1.2 con hardware flessibile per la decodifica in paralleo di video Full HD. Un totale di sei porte USB 2.0 disponibili più una porta Super Speed USB 3.0.

Piattaforma di sviluppo USB 3.0

Cypress Semiconductor ha presentato una piattaforma di sviluppo a basso costo, semplice da usare, che permette ai progettisti di aggiungere alte prestazioni USB

3.0. Il nuovo SuperSpeed Explorer Kit si basa su un controller programmabile USB 3.0 EZ-USB FX di Cypress, che offre la flessibilità necessaria per affrontare una vasta gamma di applicazioni.
EZ-USB FX3 è dotato di una interfaccia programmabile altamente configurabile (GPIF II), che può essere programmato in configurazioni a 8, 16 e 32 bit. GPIF II FX3 permette di comunicare direttamente con i processori applicativi, FPGA, supporti di memorizzazione, e sensori di immagini, fornendo una velocità di trasferimento dati fino a 400 Megabyte al secondo.
Il core CPU on-chip ARM9 con 512 KB di RAM offre 200 MIPS di potenza di calcolo, ed è disponibile per le applicazioni che richiedono l'elaborazione di dati locali
Il kit comprende anche un debugger integrato con un'interfaccia USB standard per semplificare ulteriormente i design e accelerare il time-to-market.

FP Web Server

L'offerta commerciale di Panasonic Electric Works Italia per le soluzioni industriali in cui sia richiesto il controllo e la programmazione remota si articola in moduli con flessibilità totale sia per il collegamento a una rete cablata (Ethernet, Intranet o Internet, su linea analogica PSTN) sia per la comunicazione mediante soluzioni wireless (GSM,GPRS,HSPA).

Il cuore del controllo non risiede nel solo plc ma è condiviso con il modulo FP Web Server di Panasonic; tale unità permette di gestire i dati del plc sia in lettura che in scrittura mediante pagine HTML o codice Java Script con tecnologia Ajax. È inoltre possibile inviare e-mail in base a un determinato evento con allegati i dati del PLC. FP Web Server permette di dialogare sfruttando il protocollo standard Modbus TCP (Server e Client) che garantisce ampie possibilità di comunicazione tra PLC di marche diverse e dispositivi di controllo per realizzare il M2M (machine to machine). Nel campo del telecontrollo sono inoltre disponibili i protocolli IEC60870-5-104 e SNMP. Questi protocolli possono essere appoggiati a una rete Open VPN per realizzare una VPN criptata e gestire l'infrastruttura in maniera del tutto trasparente all'utilizzatore.

Mostre Convegno 2015

10 marzo 2015
MC4-Motion Control for 2015

MC4 MOTION CONTROL

Data da segnare in agenda! Impossibile mancare all'edizione 2015 di MC4-Motion Control for che in questi anni si è sempre confermata essere l'appuntamento di riferimento per chi vuole conoscere in modo approfondito tutte le tecnologie per il controllo del movimento al servizio di macchine e impianti. Un solo giorno, una vera full immersion.

18 giugno 2015
ITE Day – Industrial Technology Efficiency Day 2015

INDUSTRIAL TECHNOLOGY EFFICIENCY DAY

Dopo il riscontro positivo registrato da parte delle aziende espositrici e dei partecipanti, Fiera Milano Media propone in linea con la scorsa edizione una sessione plenaria realizzata con l'autorevole contributo di Business International, le sessioni di presentazione dei prodotti ad opera delle aziende espositrici e i **laboratori** organizzati dalle Redazioni in collaborazione con primarie aziende del settore durante i quali i visitatori potranno imparare veramente qualcosa sui prodotti, come utilizzarli, e come realizzare vere e proprie applicazioni sotto la guida di esperti.

15 ottobre 2015
S&PI – Sensors and Process Instrumentation 2015

S&PI SENSORS & PROCESS INSTRUMENTATION

Unica mostra convegno dedicata all'automazione, alla sensoristica e alla strumentazione di processo, S&PI si presenta quest'anno con una formula rinnovata e ricca. Due le sessioni importanti: "Tech", nella quale si parlerà delle metodologie di rilevazione e misura più promettenti nell'attuale scenario tecnologico, di comunicazione, di bus di campo e wireless, e "Industry" in cui ci si focalizzerà su alcuni tra i più rilevanti settori applicativi per le soluzioni di automazione e strumentazione di processo: Oil & Gas,Acqua e Life Science.

10 dicembre 2015
Machine Automation

MACHINE AUTOMATION

L'evento quest'anno si focalizzerà sul tema del packaging con particolare attenzione ai settori applicativi del food&beverage e del life science: focus principale saranno la tracciabilità dei prodotti e l'identificazione, con interessanti excursus nel mondo della visione artificiale quale chiave di volta per migliorare la qualità dei manufatti e ottimizzare i processi in linea e a fine linea. La formula proposta è teorico-pratica: in una sola giornata si potrà partecipare alla sessione convegnistica 'tecnologica', alla parte espositiva e ai tanto attesi **laboratori**. Una modalità in grado di fare davvero 'cultura'.

Per informazioni: Elena Brusadelli Tel. 335 276990
www.mostreconvegno.it
elena.brusadelli@fieramilanomedia.it

TECH PLUS.it

EXPO MILANO 2015

FIERA MILANO MEDIA

Fiera Milano Official Partner

Riprogramma il mondo.

Fare ingegneria in un mondo complesso porta ogni giorno nuove sfide. Cambia approccio per affrontarle al meglio. Riprogramma il tuo mondo ingegneristico con la piattaforma integrata hardware e software di National Instruments. Supera la complessità dei sistemi di misura e controllo.

>> A te l'idea, a noi gli strumenti. Visita italy.ni.com

02.413091

NATIONAL INSTRUMENTS™

©2013 National Instruments. Tutti i diritti riservati. National Instruments, NI e ni.com sono marchi commerciali di National Instruments.
Altri prodotti e nomi aziendali citati sono marchi commerciali delle rispettive aziende. 14487